network diagram

Network Troubleshooting using OSI Modell

منهجيــــة حــــل
مشاكل الشبكة

الإرسال والإستقبال
مـن خلال الكابل

DNS
cache
poisoning

العدد رقم 11

NetworkSet

February 2011

NetworkSet Magazine

أول مجلة عربية مجانية تختص بأمور الشبكات

www.Networkset.net

مؤسس ورئيس وتحرير المجلة : م.أيمن النعيمي

المحررون

المهندس أيمن النعيمي
www.NetworkSet.net

المهندس أنــس الأحمــد
EE4its@hotmail.com

المهندس إســلام محمــد
Csi_Eslam@Yahoo.com

المهنـدس علاء مازن عدي
alaamazen@hotmail.com

المهندسة صفا الرمضـاني

المهنـدس نــادر المنســي
naderelmansi@gmail.com

المهندس شريــف مجـدي
sh8090@gmail.com

التصميم والإخراج الفني



Integratoin Technical Solution

eng.Anas kh Al-Ahmad

الآراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة
جميع المحتويات تخضع لحقوق الملكية الفكرية
لا يجوز النقل دون إذن من المجلة أو الكاتب

المحتويات



هي كلمة بحثت عنها كثيرا ولم أتوصل إليها إلا مؤخرا مع انها أحد الصفات التى أحب أن أوصف بها دائما إلا أن فهمتها بعد أن وصلتني رسالة من المهندسة صفا الرمضاني التى أصبحت أحد المحررين معنا في المجلة وما أعجبني في رسالتها أنها لم تكن من النوع المألوف الذي اتلقاه دوما حول الأشتراك في المجلة فعادة ماتصلني رسائل تتطلب مني الأشتراك في المجلة ويتبعها رسالة عن المواضيع التى يمكن الكتابة عنها في المجلة ويتبعها أقتراحات والخ...وهو مايسبب حيرة لي أحيانا فأنا لا أعلم أمكانية كل واحد منهم ولا مستواه الحقيقي في عالم الشبكات إلا أن المهندسة صفا خالفت كل هذه الرسائل وقامت بأرسال المقال مباشرة وطلبت مني قراءة المقال وتحديد هل هو من النوع المناسب أم لا؟!!!. وأول ما كتبته كان شكرا لكي على المبادرة الجميلة والمباشرة وهنا فقط تذكرت أن كلمة مبادرة هي الكلمة التى كنت أبحث عنها وهي ما أردت أيصاله لكم اليوم لأن المبادرة هي أكثر ما ينقصنا للأبداع والتمييز وخصوصا أن الكثير من طاقتنا العربية خامنة وتحتاج إلى من يثيرها ولو نظرنا إلى المعنى الحقيقي لكمة مبادرة في القاموس العربي لوجدنا أنها تشير إلى الأسراع في عمل ما بدون مماطلة وهذا أن كان يدل على شيء فهو يدل على العمل الجاد والرغبة في تنفيذ شيء ما أما المماطلة فهي تدل على شيء واحد وهو الكسل والخمول ولأطرح عليكم مثال عملي أجده تقريبا كل أسبوع على المنتديات العربية ويفشل فشلا زريعا.

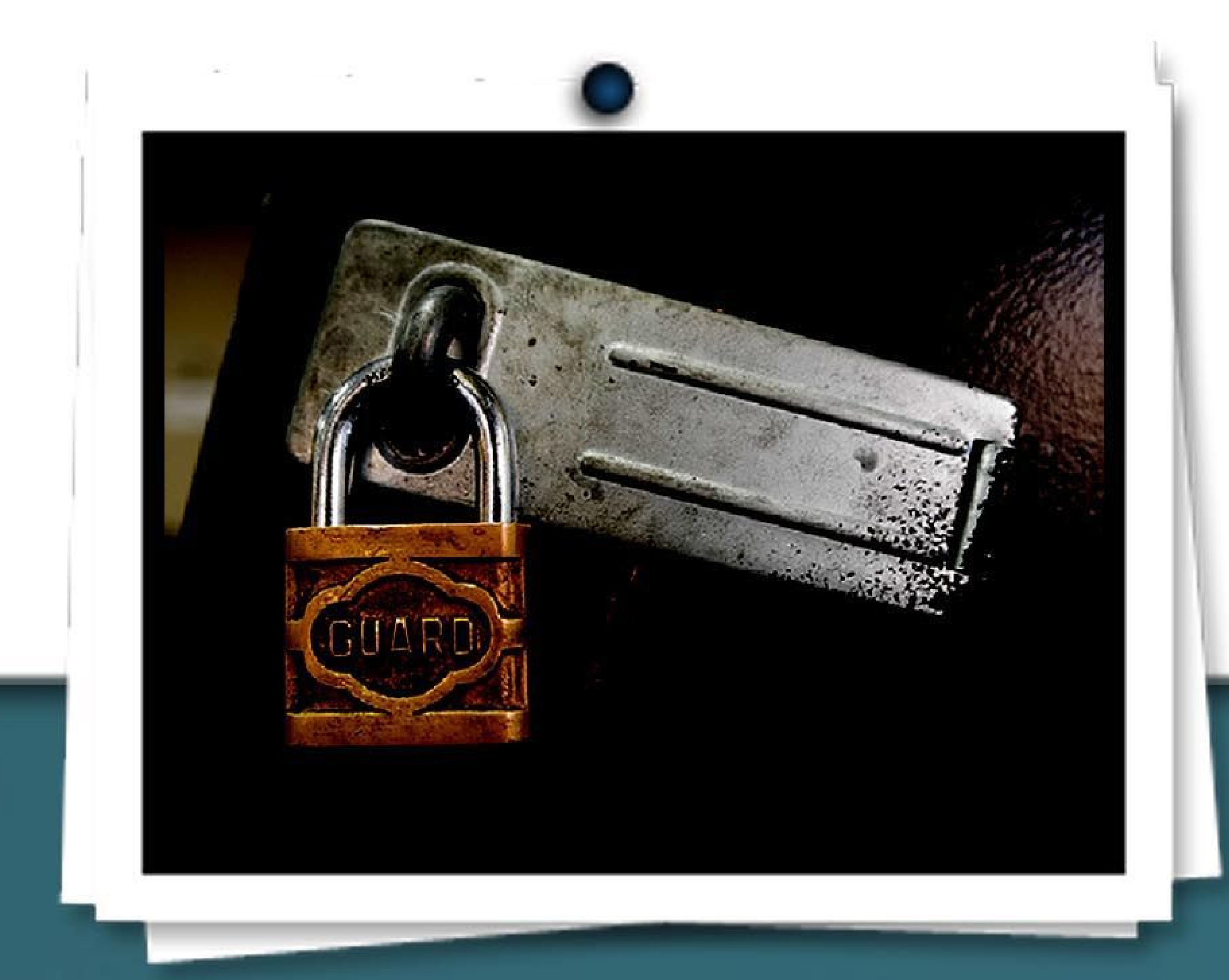
تفتح المنتدى وتجد موضوع عنوانه كالآتي " كل واحد يقوم بوضع معلومات عن كوابل الشبكات " أو " الموضوع الأوحد لكل المشاكل التى تمر بك في الحياة العملية " فكرة هذه المواضيع جميلة لكن لو فتحت ونظرت ماهو مكتوب بها لما فتحتها مرة أخرى فعلا سبيل المثال تجد أن الموضوع الاول يملك أكثر من عشرين رد وكلهم يؤيد الفكرة وهناك من يشكر صاحب الموضوع على الفكرة الجهنمية وهناك من يقول بأنتظار باقي الأعضاء والكل يجلس ينتظر أصحاب الخبرات العالية والأشخاص الذين ولدوا وهم يحملون كابل للشبكة ويختفي الموضوع بعد أسبوع لتنتهي معه حكاية كوابل الشبكة . من وجهة نظري هذه الافكار يجب أن تموت لأن الشخص الذي بادر وكتب هذا الموضوع لم يعمل فيه فهدفه سلبي وهو معرفة أنواع الكوابل فقط من خلال موضوع وهمي يذكر فيه أنه لأفادة الآخرين والحقيقة غير ذلك والسبب لأنه لم يبادر بكتابة أي كلمة تفيد الموضوع ونفس الشيء يحدث مع باقي المواضيع فهي تحتاج من صاحبها أن يكون من اكثر الناس مساهمة فيه وليس متفرج يملك أفكار وهمية وخصوصا أن الأفكار والمواضيع كثيرة ولكن جميعها تنتظر مبادر حقيقي لكي يطرحه وليس مستهلك ذو عقلية متحجرة .

الخلاصة التى أريد أن أوصلها لك أخي القارئ كن مبادر ومبادر أيجابي وأعمل وأجتهد حتى تصل إلى مبتغاك ولا تكن مجرد نقطة على السطر توضع في أخر الكلام وحاول أن تشعر دائما بمثل ما أشعر عندما أطرح على نفسي السؤال الصغير أين نحن والغرب أين ؟؟؟ هل ياترى أن بأمكانني أن أثبت للعالم أننا لسنا مستهلكين ؟؟؟ هل أنا قادر على التغيير ؟؟؟ كل هذه الأسئلة لا تقرأها مجرد قرأه بل أشعر بها وعندها سوف تأخذ الطاقة التى سوف تجعلك مبادر حقيقي وإيجابي.

أنطلق مشروعي الجديد لعمل أكبر موسوعة عربية في الشبكات وهي مبادرة جديدة مني لتغيير الواقع والمحتوى العربي وهي تحتاج إلى الكثير من المبادريين لأنجاحه لكن أن لم أجد من يبادر ثقوا أن هذه الموسوعة لن تتوقف يوما واحدا عن الأتساع أن شاء الله .

أيمن النعيمي

5 Step secure Cisco



على نفس الأسلوب الذي أتبعته من قبل في طرحي لموضوع خمس خطوات يجب أن تعرفها حول سويتشات سيسكو أعود إليكم لكي أستعرض معكم أهم خمس خطوات يجب على مدير الشبكة أتخاذها لتأمين الشبكة التى تستخدم أجهزة سيسكو ومما لاشك فيه أن خطوات الحماية أكثر من هذا بكثير إلا أن هذه الخطوات تعتبر هي الأساس في عملية حماية الشبكة والأجهزة الموجودة عليها .

الخطوة الأولى

تشفير كلمة السر الخاصة بالدخول على الروتر

يصاب الكثير من المبتدئين في عالم سيسكو بالأرتباك بين امر الـ Enable Password وأمر الـ Enable secret Password والفكرة ببساطة تقول أن كلمة السر هذه هي للمكان نفسه وهي تستخدم للدخول إلى الروتر أو إلى السويتش ولكن الفرق بينهما أن الاولى لاتشفر عند عرض الأمر Show Run بينما كلمة السر الخاصة بالأمر الثاني يتم تشفيرها ومن الصعب جدا كسرها ولو في حال قمنا بكتابة كلا الأمران فأن الروتر سوف يأخذ كلمة السر الثانية الخاصة بي الـ Secret Password لذلك أول خطوة سوف نقوم بها هي وضع كلمة سر من النوع المشفر من خلال الأمر التالي :

```
Router(config)# enable secret your password
```

الخطوة الثانية

تشفير كل كلمات السر

عندما نقوم بعرض الأعدادات الموجودة على الروتر من خلال الأمر Show Run سوف نلاحظ أن كل كلمات السر الموجودة غير مشفرة ماعدا الـ Secret التى تحدثنا عنها من قبل أما باقي الكلمات فتكون كلها Clear Text وهذا يشمل كلمة السر الخاصة بالتلنت والكونسول والأكسيلاري والـ Enable Password لذلك تعتبر خطوتنا الثانية هي تشفير هذه الكلمات من خلال كتابة الامر التالي في الـ Configuration Mode :

```
Router(config)# service password-encryption
```

الخطوة الثالثة

تحديد كلمة سر خاصة بالكونسول.

يعتبر منفذ الكونسول سلاح ذو حدين فهو المنفذ الوحيد الذي يمكن من خلال أسترجاع كلمة السر للدخول إلى الروتر وفي نفس الوقت يكون غير محمي بأي كلمة سر عند أستخدامه لأول مرة لذلك خطوتك الثالثة سوف تكون حماية منفذ الكونسول من الأشخاص الغيورين والذين يتربصون بك في مكان العمل وذلك من خلال الأوامر التالية :

```
Router(config)# line con 0
Router(config-line)# login
Router(config-line)# password your password
```

أيمن النعيمي

الخطوة الرابعة

تفعيل بروتوكول الـ SSH

يقع أكثر من سبعين بالمئة من مهندسي ومديري الشبكات في خطأ فادح وهو أستخدام التلنت للاتصال مع الروتر, فكما نعلم أن أغلب الأجهزة وان لم يكن كلها يحتاج منا الأتصال بها عن بعد للأطلاع عليها وعمل بعض الأعدادات لذلك يلجأ الأغلبية إلى تفعيل بروتوكول التلنت لهذه المهمة وهو أحد أكثر الاخطاء شيوعا لأن التلنت ببساطة لايقوم بتشفير اي شيء أثناء الأرسال والأستقبال ومن بينها كلمة السر والأوامر والذي يجعلها عرضة لأي عملية تجسس لذلك خطوتك الرابعة هي تفعيل بروتوكول الـ SSH عوضا عن التلنت والذي يعرف بانه يقوم بتشفير عملية الاتصال بشكل كامل والاعدادت على الشكل التالي :

```
Router(config)# ip domain-name My Domain
Router(config)# crypto key generate rsa
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password your password
Router(config-line)# transport input ssh
```

الخطوة الخامسة

تأمين المنافذ الموجودة على السويتش

في أحصائية قرأتها منذ فترة تبين أن تسعين بالمئة من السويتشات الموجودة على الشبكة منافذها الغير مستخدمة تعمل ولم يتم أيقافها وهي أيضا أحد الأخطاء الشائعة جدا عند مهندسي أجهزة سيسكو لذلك خطوتك الخامسة سوف تكون أطفاء كل المنافذ الموجودة على السويتش من خلال الدخول على المنفذ وكتابة الامر Shutdown

إلى نكون قد أنتهينا من حديثنا وأرجع وأقول أن الخطوات الخاصة بتأمين الشبكات أكثر من ذلك بكثير لكن تعتبر هذه الخطوات من الأشياء التى يجب أن تقوم بها أولا وبعدها تفكر في الخطوات الثانوية والتى من بينها أعداد الـ Vlan والـ Port Security والخ... أتمنى أن تكونوا قد استفدتوا وأن أكون قد وفقت في أيصال المعلومة ودمتم بود

Mikrotik Router OS

لا اعرف كيف ابداء الكلام او من اين حيث ان الكل يعرف الاحداث التى مرت بها مصر ومازلت تمر بها وموضوع الانترنت والاتصالات التى تم قطعهما بالكامل وعزلنا عن العالم كله وكننا فى داخل زجاجه وهو السبب الرئيسى فى تاخير استكمال المقالات فكل المصريون وانا اولهم نمر باصعب الظروف التى لم تستطع اقوى اجهزة المخابرات والامن فى العالم كله التنبوء بها وهانحن الان نحاول ان نخرج من عنق الزجاجه...

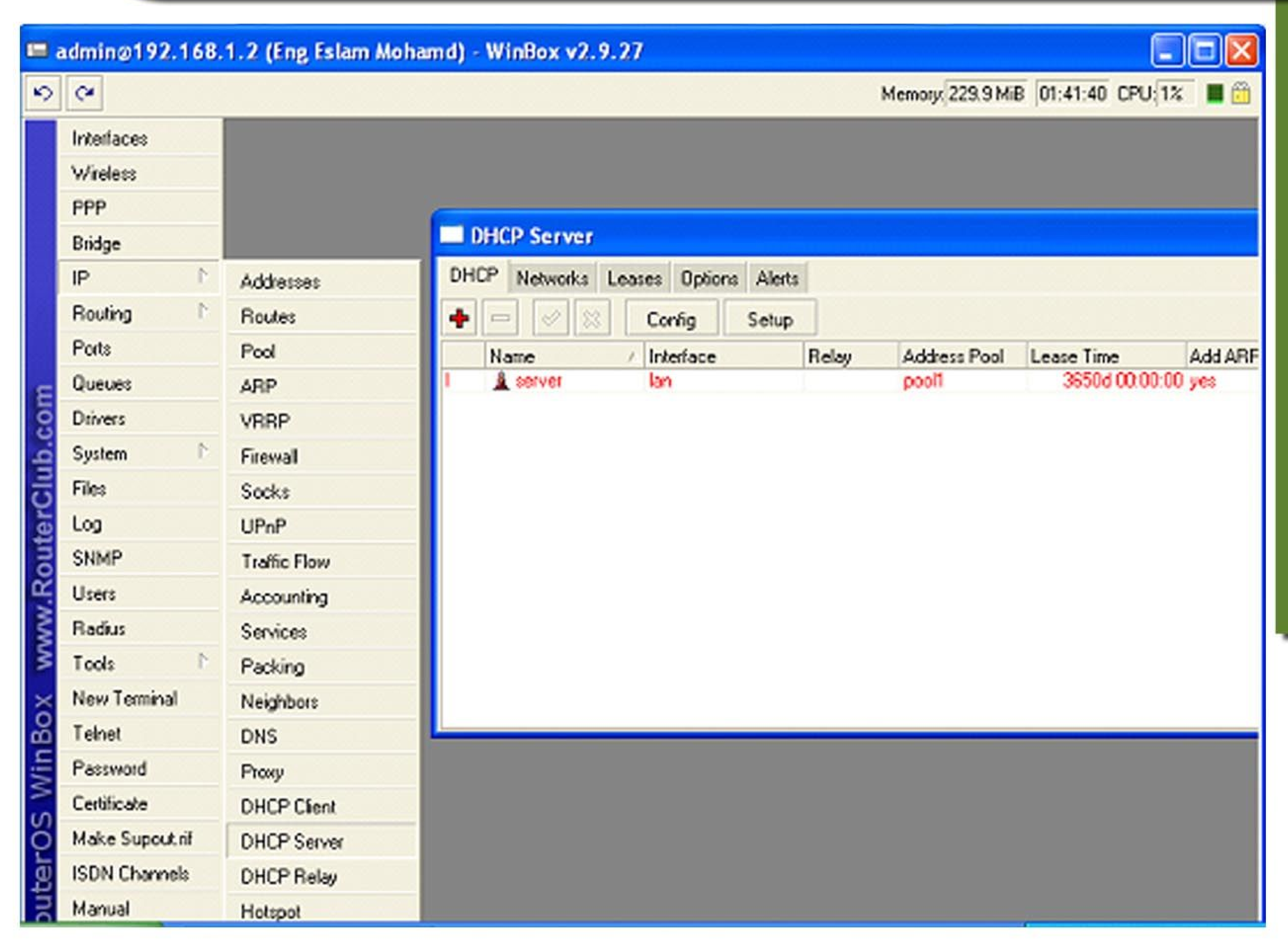
Eng. Eslam Mohamed

اليوم سوف نستكمل معا الموضوع الذى بدناه عن المايكروتك ولكن اليوم اود ان اقول لكم ان المايكروتك كان يعيش مع المصرين فى الاحداث الحاليه !!!!!! طبعا الكل يتسال الان كيف هذا ؟؟؟؟!! نعم ان المايكروتك كان له دورا كبيرا اثناء انقطاع الانترنت حيث ان الانترنت كان يعمل فقط من خلال التليفون الارضى او مايعرف بخدمه الديل اب (Dial up) والذى قد اختفى منذ زمن بعيد ولم يبقى اى كروت (فاكس مودم) موجوده بالاسواق او حتى البيوت الا عند القليل من البعض والذين لم يقومون بتحديث اجهزتهم او مازلوا يحتفظون بها .

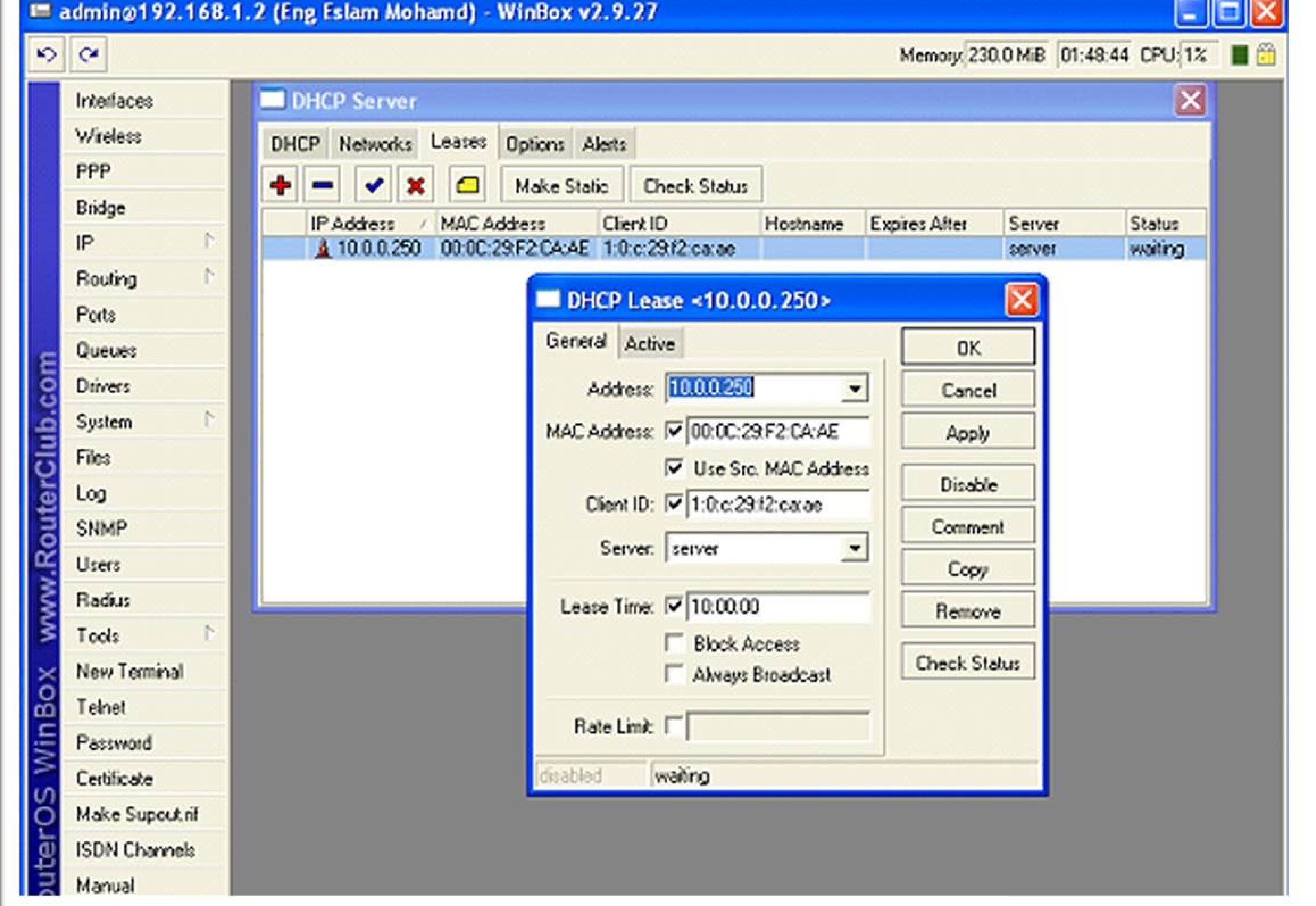
عند قطع الانترنت لم يكن هناك اى وسيله اتصال بالانترنت الا من خلال (الفاكس مودم) وهى الثغره التى لم يكن يعرفها الكثير من الناس او حتى يتوقعها متخذى القرار ولكن ماهو دور المايكروتك ؟؟!! لقد قام البعض باستخدام خط التليفون الارضى كخط بديل لخط الانترنت اى هو البديل للكبل القادم من الروتر وتم ادخاله على المايكروتك ليقوم هو الاخر بجانبه بمعالجه الترافيك واخراجه الى العملاء مع اعاده توزيع الاشاره او الترافيك القادم من النت طبعا هذا كان الحل الوحيد فى ظل عدم وجود الانترنت والكل يعلم طبعا مدى البطى الخاص بسرعه الفاكس مودم ولكن لم يكن لدينا اى خيار اخر وهكذا وقف المايكروتك بجانب الشعب المصرى .

دعونا الان نتطرق لاهم ميزة فى المايكروتك بل الاهم لاى شخص مهتم بمجال الاى تى او تكنولوجيا المعلومات الا وهى ال Authentication , اولا تعريف هذه الكلمه هى باختصار شديد تعنى الحقوق التى يتم السماح بها او الصلاحيات المخصصة لكل شخص وبكلام أخر هل هذا الشخص له الحق فى الدخول على الانترنت مثلا ام ليس له الصلاحيه واذا كانت له هذه الصلاحيه هل له الحق فى الدخول على كل المواقع ام هناك مواقع محجوبه او اننا نريد فقط ان يدخل هذا الشخص على مواقع معينه فقط , كل هذه الاشياء تسمى Authentication او صلحيات .

ان المايكروتك يسمح لنا باختيار الاسلوب الذى من خلاله نعطى الصلحيات او نقرر من هم الاشخاص المسوح لهم بالدخول على الانترنت او حتى الشبكه اولى هذه الطرق اننا يمكن ان نقوم بتفعيل ال DHCP SERVER تلك السيرفر التى تقوم بتوزيع الايبيهات بشكل اتوماتيكى وعشوانى على المستخدمين



ولكن اذا تمكننا من معرفه الماك ادرس MAC لكل العملاء بالشبكه فيمكننا ربط الاى بي الخاص بكل عميل الذى يقوم بتوزيعه ال DHCP SERVER بالماك ادرس وبالتالى فان الكلاينت عندما يقوم بتشغيل الجهاز سوف يقوم بعمل Broadcast على الشبكه لمعرفه ال DHCP SERVER ثم يقوم بطلب الاى بي منه فان السرفر هنا يتاكد اولا من الماك ادرس الخاص بكارته الانترنت عند الكلينت فاذا كان هو نفس الماك الموجود بالسرفر يقوم حينها باعطاء الاى بى الذى قمنا بتحديده , طبعا هذه ميزة قويه جدا!!! حيث اننا اجبرنا العميل على اخد اى بى معين وكانه اى بى ثابت (static ip) وليس اتوماتيك (dynamic ip) رغم انه لم يقوم بنفسه بكتابه الاى بى على جهازه وليس هذا فقط بل اننا يمكنن ان نجعل هذا العميل يحتفظ بهذا الاى بى لاى فتره نريدها مهما كانت حتى نقوم نحن بالتعديل بها بعد ذلك وهنا نكون قد منعنا مشكله الكونفليك فى الاى بى ومشكله المثلث الاصفر ...

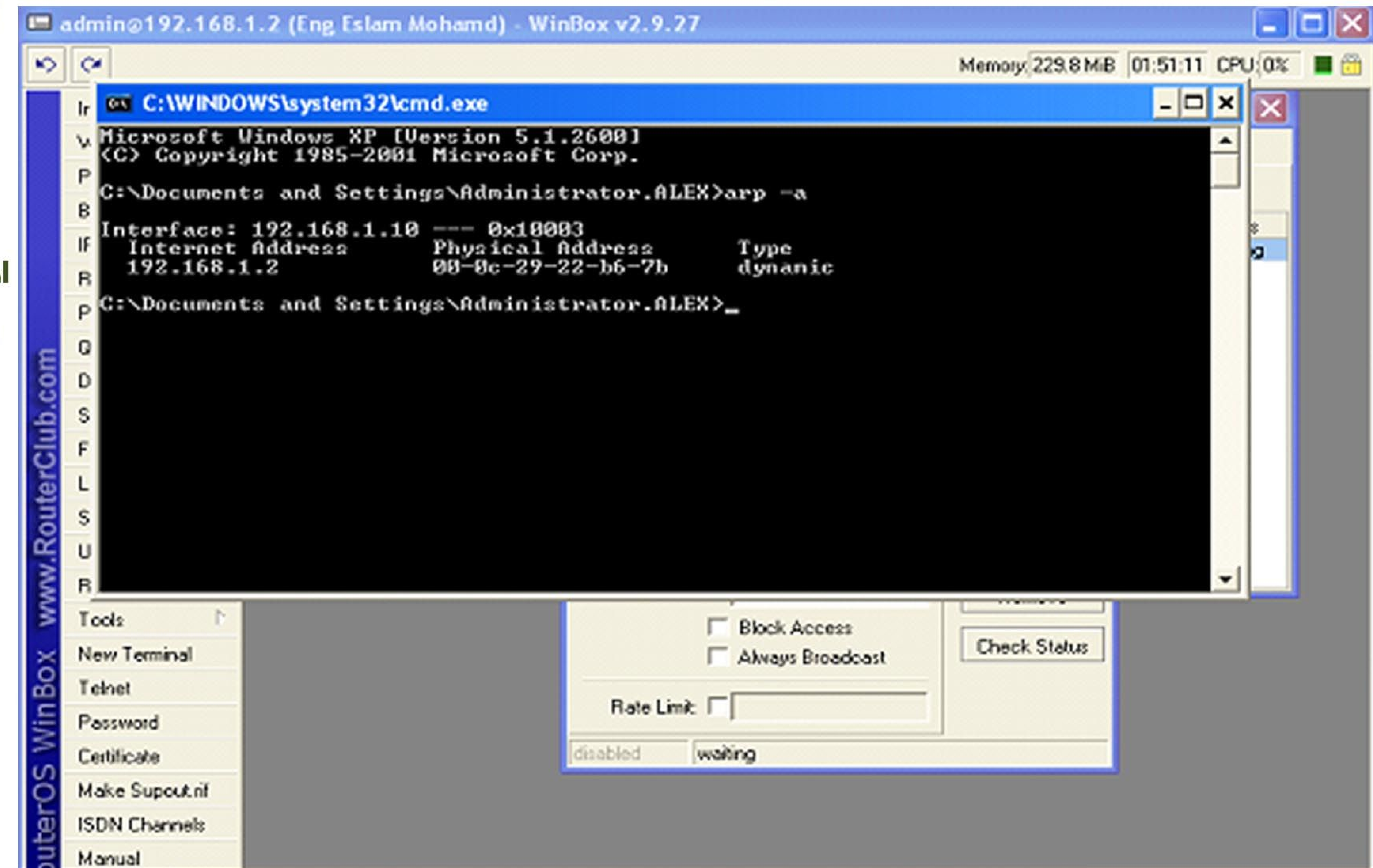


هناك سؤال الان قد ياتى ببال البعض ماذا لو لم يكن الماك ادرس معنا هل سوف ياخد الكلاينت اى بى ويتصل من خلال السرفر فالحقيقه نعم ولكن يمككنا ايضا التغلب على هذه المشكله بكل ببساطه حيث ان لكل جهاز مربوط بالسرفر هناك ما يسمى بجدول الارب كاش Arp وهو جدول موجود بالسيرفر حيث ان اى عميل يقوم باخد اى بى يكون امامه الماك ادرس الخاص به كما يمكن مشاهده هذا الجدول من الاتى

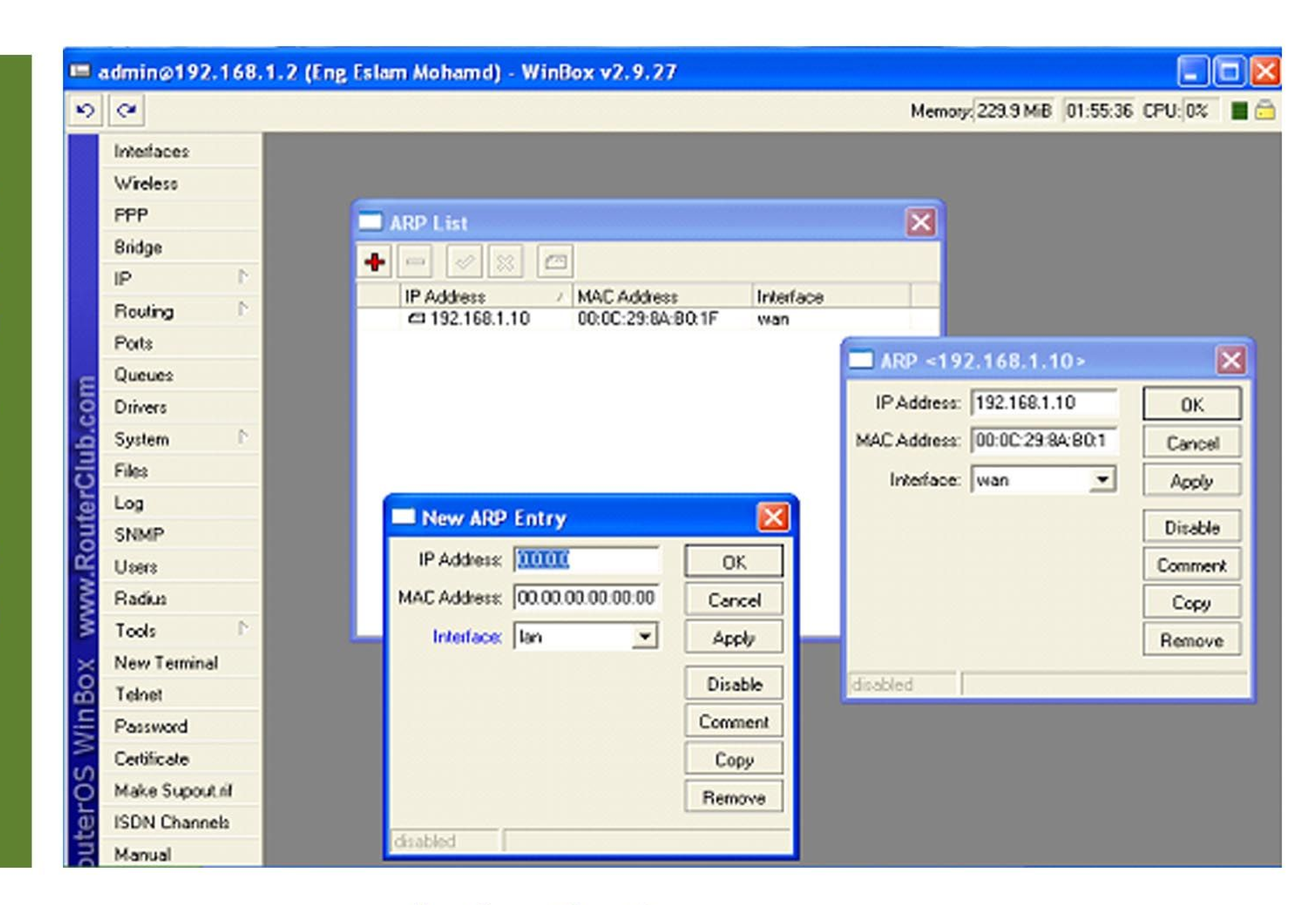
ندخل على cmd ---- run --- stat ----

ومنها نقوم بعمل بينج على اى بى موجود معنا فى الشبكه او الجيت واى الموجود وليكم على الشكل التالى ping 192.168.1.254 بحيث تكون هناك استجابه ثم نقوم بكاتبه الامر التالى arp –a لنلاحظ وجود الاى بى وامامه الماك ادرس الخاص به

ومن هنا اذا كان الاى بى صحيح بما انه اخد من السيرفر DHCP SERVER والماك صحيح يتم الولوج الى السيرفر وانشاء الاتصال والدخول على الانترنت ولكن اذا كان الماك غير صحيح لن يتم ذلك وهو ما سوف نقوم بعمله على السيرفر حيث اننا سوف نقوم بملىء الجدول الخاص بالارب بشكل يدوى حيث سوف نقوم باضافه كل الرنجات التى يقوم DHCP SERVER بتوزيعها وربطها بماك ادرس غير صحيح او اصفار كما يقوم البعض



Mikrotik Router OS



وعندها الكلينت سوف يحصل على اى بى لكن الماك غير صحيح فهو غير مطابق للماك الموجود بالسرفر حينها سوف لن يتم الاتصال وهى احدى اساليب الحمايه الموجود بالمايكروتك.

ايضا من هذه الطرق ان تكون ال Authentication من خلال يوزر نيم وباسورد وهدى الطرق للذين يقومون باستخدم طريقه ال hotspot فى الاتصال او pppoe وهى الطرق التى يتم من خلالها ادخال اسم مستخدم وكلمه سر اما فى شاشه لوجن او صفحه متصفح html كما نلاحظ من الصور

E:\Image\FULL MikroTik CD\الساحر سبوت\hotspot\login.html

File Edit View Favorites Tools Help

الساحر لجميع خدمات الكمبيوتر

بيع - شراء -استبدال -صيانه - تجميع - شبكات

المندره قبلي -٢١ ش المدارس بجوار مدرسه سعد زغلول

خدمة ٢٤ ساعة

login $(username)

password

OK

:: للدعم الفنى ::

010 6449212

:: تحذيرات ::

الرجاء الألتزام بميعاد تسديد الأشتراك

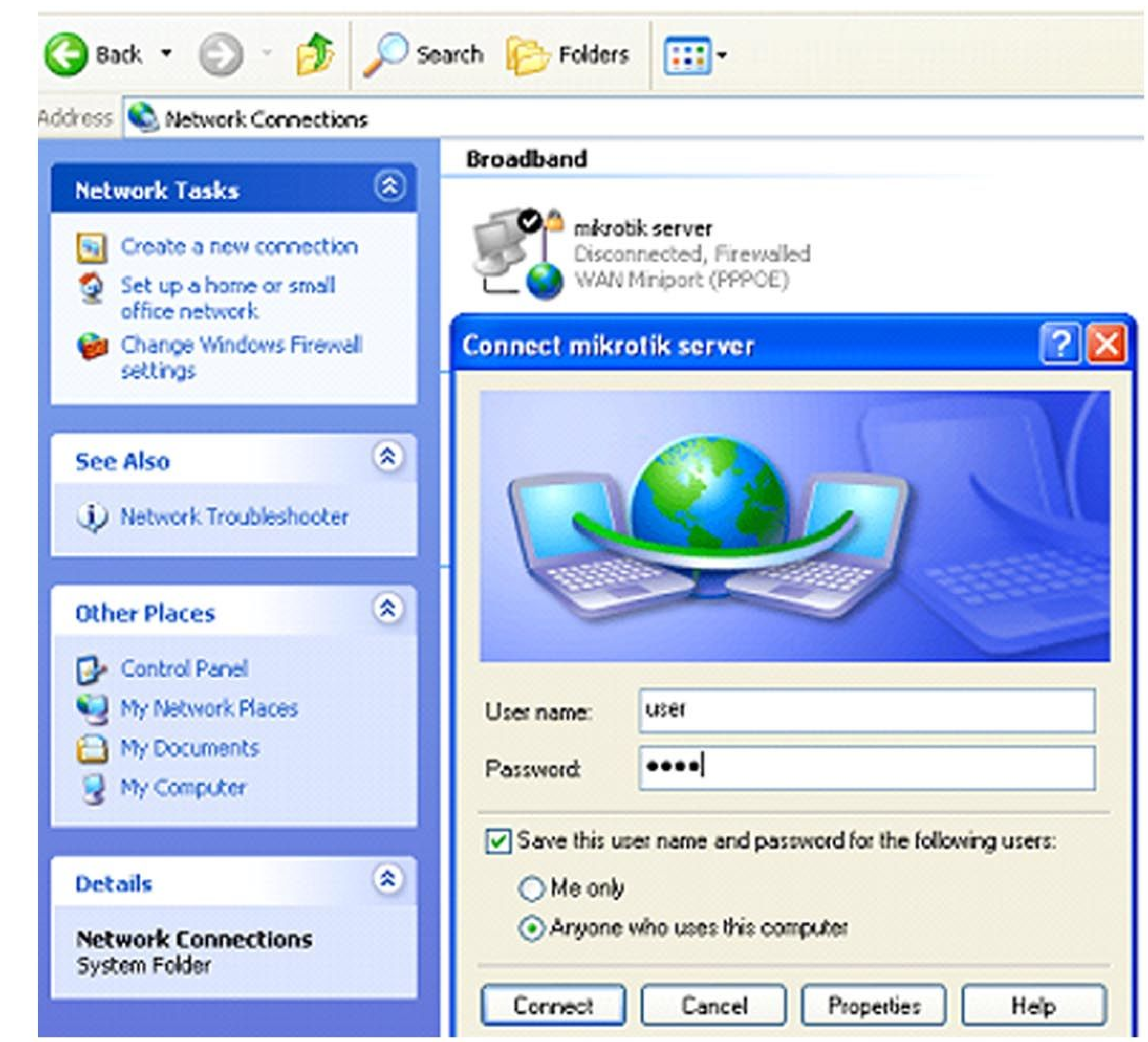
الرجاء عدم تغير الIp الخاص بك

الرجاء تثبيت برنامج حماية تثق فيه على جهازك للحفاظ على بياناتك

فى حالة نسيان اسم الدخول او كلمة المرور الرجاء الأتصال بأدارة الشبكة فى اقرب وقت

Designed by: Eng Eslam Mohamed © 2010 Eng Eslam Mohamed - 0102256465 - CSI_ESLAM@YAHOO.COM All Rights Reserved

وهى من بعض السيرفرات حيث ان عمليه Authentication تتم من خلال اسم مستخدم وكلمه سر , وليس ذلك فقط بل اننا يمكننا التحكم فى الكلاينت صاحب كلمه السر بمعنى هل من الممكن ان يستخدم كلمه السر واسم المستخدم من اى جهاز على الشبكه ام من على جهاز معين حيث ايضا يمكن ربط الاى بى او الماك ادرس او الاثنين معا باسم المستخدم وكلمه السر



نكتفى اليوم بهذا القدر وعلى وعد باستكمال باقى الحلقات فى الاعداد القادمه باذن لله لنتعرف اكثر على اهم الخدمات التى يقدمها المايكروتك



DNS cache poisoning

صفا الرمضاني

عادة

عندما نبدا تصفح المواقع تبدأ العملية من خلال كتابة أسم الموقع أولا ولكن مثلا موقع networkset.net نجد أن الموقع قد فتح ومن دون ان نشعر بأي شيء حدث.

وحقيقة عملية طلب الموقع تمر بمرحلة خفية تجري بدون ان نشعر بها وهي عملية الـ DNS Resolving تقوم هذه العملية ببساطة على ترجمة أسم الموقع networkset.net إلى الأيبي وطبعا هذه العملية مهمة كوننا نعلم أن كل مايجري من خلال الشبكات يتم من خلال الأرقام فقط وليس العنوان وتعتمد هذه الاجهزة في عملية الترجمة على سيرفرات تعرف بي DNS أو Domain Name Server وما قد لانعرفه أيضا أن عمليات الترجمة هذه تحفظ في جداول مؤقتة في ذاكرة الجهاز وتزول مع أول عملية أعادة أقلاع للجهاز وهي مهمة حتى يعود لها الجهاز مرة أخرى لو في حال طلب مستخدم الجهاز الموقع ذاته.

لنلقي نظرة اكثر قربا على كيفية تحليل العناوين عندما نقوم بطلب اسم موقع فإن اول خطوة تتم هي علمية تحليل العنوان وذلك بالبحث في الجدول الموجود في الـ resolver والذي يضم اسماء وعناوين المواقع التي تم فتحها مؤخرا ، كما في الصورة المجاورة :

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Safa>ipconfig /displaydns

Windows IP Configuration

    api.yontoo.com
    ----------------------------------------
    Record Name . . . . . : api.yontoo.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 729
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 38.107.189.4


    www.google.com
    ----------------------------------------
    Record Name . . . . . : www.google.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 90
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : www.l.google.com
```

الهجوم

هناك عدة اسباب تجعل المهاجمين يقومون بشن هجماتهم على الـ DNS server سأذكر الاسباب الرئيسية لمثل هذه الهجمات :

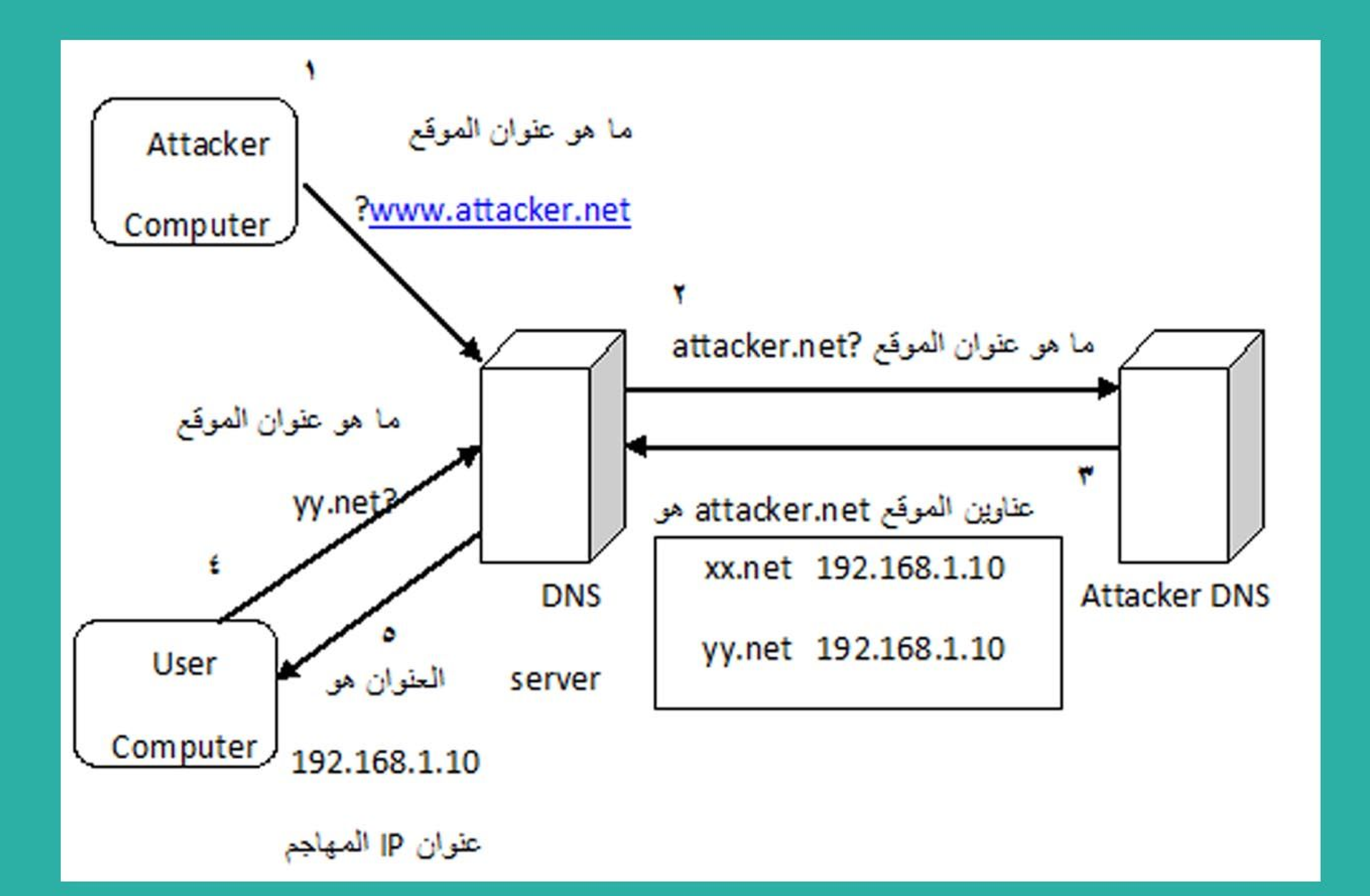
1_ سرقة الهوية identity theft

2_ نشر الـ malware

3_ نشر معلومات خاطئة ومغلوطة

4_ السبب الرابع هو ما يعرف بـهجمات man _in_the_ middle .

فكرة الهجوم تقوم على تبديل وتزوير عنوان الموقع ، فمثلا لو قام المستخدم بطلب عنوان الموقع good.com والذي عنوانه 203.193.14.103 فإن الهجوم سيتسبب بإرجاع العنوان 209.186.22.90 والذي هو عنوان موقع المهاجم . والشكل المجاور يوضح ألية الهجوم :



(نلاحظ ان الـ Attacker DNS server قد يعيد نفس العنوان لأكثر من موقع وكلما تم طلب احد هذه المواقع سيتم اعادة العنوان المزور وبالتالي سيزداد عدد الضحايا) .

عندما يستلم الـ local DNS الرد من سيرفر المهاجم (الذي يظهر ويدعي انه السيرفر الموثوق) فإن عنوان الـ IP مع اسماء المواقع سيتم حفظهم في الـ local DNS cache ومن ثم يرسل العنوان إلى الـ DNS resolver وبالتالي سيكون كل من الـ local DNS والـ resolver مصابين ، فعندما يقوم اي جهاز في هذه الشبكة بطلب هذا الموقع فإن الـ DNS server سيقوم بإرسال عنوان موقع المهاجم ، وهكذا تبقى الإصابة إلى ان تنتهي فترة الـ Time to live الخاصة بهذا الموقع فيتم حذف العنوان من الجدول او الـ cache .

فإذا وجد عنوان الموقع فسيعيد النتيجة أما إذا لم يجده في الجدول فإن الـ DNS resolver سيقوم بإرسال طلب إلى الـ local DNS والذي بدوره يقوم بالبحث عن العنوان في الـ cache الموجود فيه فإذا وجد النتيجة سيقوم بإرسالها الى الـ DNS resolver اما إن لم يجده في الـ cache فإنه يقوم بإرسال الطلب الى الـ root DNS وهكذا إلى أن يحصل على رد بعنوان الموقع المطلوب وبالتالي فإن الـ local DNS سيقوم بحفظ اسم الموقع وعنوانه في الـ cache الخاص به ومن ثم ارسال اجابة للـ DNS resolver بعنوان الموقع ، والأخير سيقوم بحفظ العنوان في الجدول الخاص به والاتصال بالموقع المطلوب من خلال عنوانه .

(في حال عدم الحصول على عنوان الموقع فهذا يعني أن الموقع غير موجود على شبكة الانترنت) .

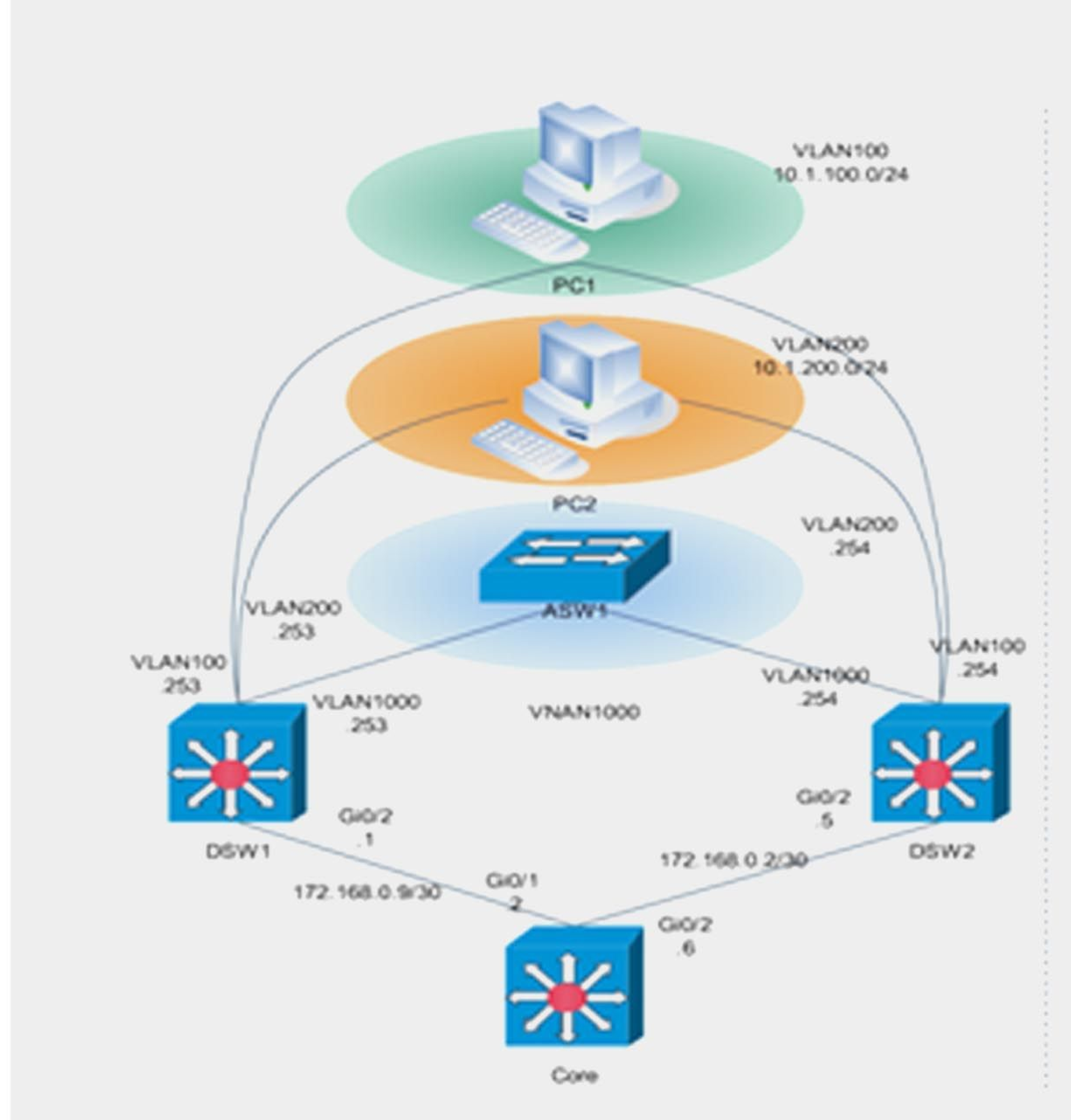
الحماية

هناك عدة امور تقلل من خطر هذه الهجمات ، فمثلا استخدام احدث اصدارات برامج الـ DNS مثل برامج الـ BIND والـ DNSSEC (Domain Name Security Extensions) والذي يعد افضل من سابقه وأقوى وأكثر أمانا (حيث ان هذه البرامج تقوم بعمل فلترة للردود المستلمة ورفض اي عناوين اضافية وتتبع أليات متطورة في عملية ارسال واستقبال الاستفسارات) ، وايضا من طرق تقليل الهجوم فصل الـ external DNS server عن الـ internal DNS server ، والتأكد من موثوقية ومصداقية السيرفر الذي يرسل الإجابة ، وكذلك إخفاء رقم اصدار البرامج المستخدمة يساعد على تخفيف الهجمات ، وإزالة الخدمات غير الضرورية من الـ DNS server ، ويفضل استخدام البرامج احادية المهمة عن البرامج متعددة المهام .

اسأل الله أن اكون وفقت في الطرح ، وإن اصبت فمن الله وإن اخطأت فمن نفسي ، والسلام عليكم ورحمة الله وبركاته .

أهم البرامج الخاصة بتصميم وتوثيق الشبكات

مقالتي لهذا العدد سوف تتحدث عن أفضل البرنامج المعتمدة للقيام بعمل مخططات أو Diagram للشبكة من أجل توثيقها والأطلاع عليها وقت الحاجة لان وجودها يعتبر أحد أهم الأشياء التى تساعد مدير الشبكة على فهم الشبكة التى لديه وكيف تعمل والتى يلجأ لها دائما لحل أي مشكلة تواجهه في الشبكة لأنها ببساطة تقدم له كل المعلومات اللأزمة لبدأ عملية الـ Troubleshooting على الشبكة.



البرنامج الأول

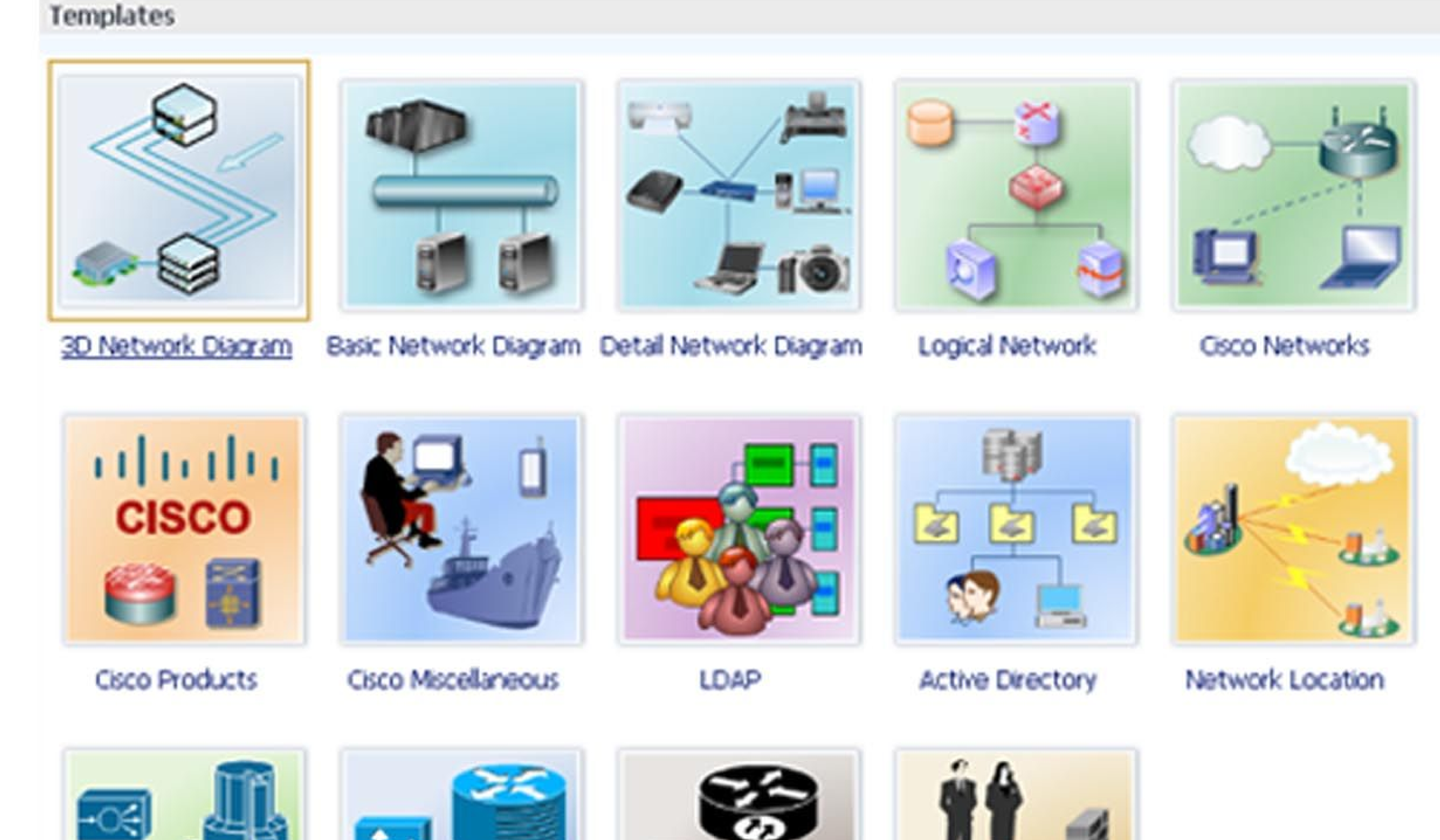
Edraw Network Diagram 5.2

شهرة هذا البرنامج لاتقل عن شهرة البرنامج الأول وأمكانياته كثيرة أيضا في مجال الشبكات وهو أيضا برنامج غير مجاني وثمنه 69 دولار ومن مميزاته الجميلة امكانية عمل مخطط بشكل ثلاثي الأبعاد بالأضافة إلى دعمه للأجهزة الخاصة بسيسكو وهذه صورة توضيحية

بالنسبة لي تعاملت مع هذا البرنامج أكثر من الأول وأعجبني اكثر البرنامج ياتي تجريبي ولمدة 30 يوم تستطيع تحميله من موقع البرنامج على الرابط التالي:

http://www.edrawsoft.com/download.php

للقسم المخصص للشبكات .





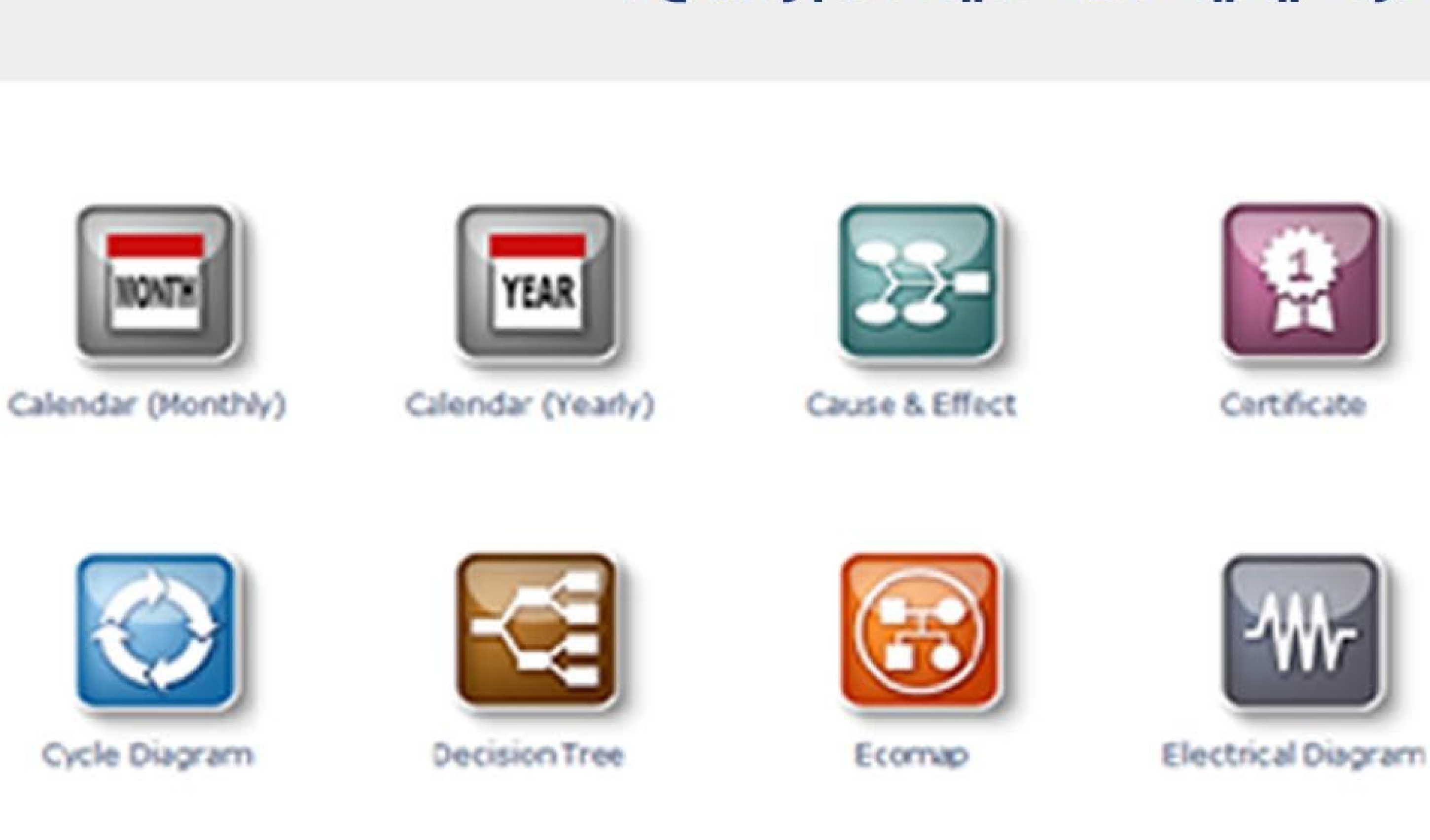






البرنامج الثاني
SmartDraw 2010

أحد أشهر وأفضل البرامج الموجودة في هذا المضمار وهو برنامج غير مجاني وثمنه 179 دولار وهو برنامج ضخم جدا بأمكانياته فهو يتيح لك عمل رسومات ومخططات للعديد من الأشياء وليس فقط للشبكات بالأضافة إلى أمكانية حفظ المخطط على شكل صورة أو ملف PDF أو HTML أو للأوتوكاد وهذه صورة توضيحية لأمكانيات البرنامج .







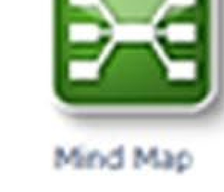
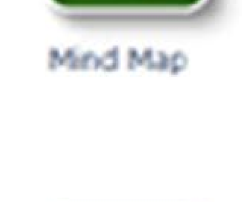








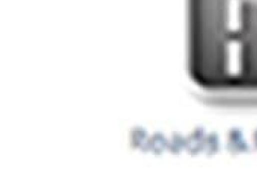


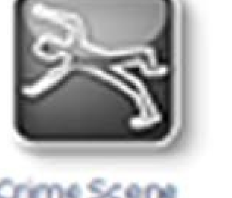
















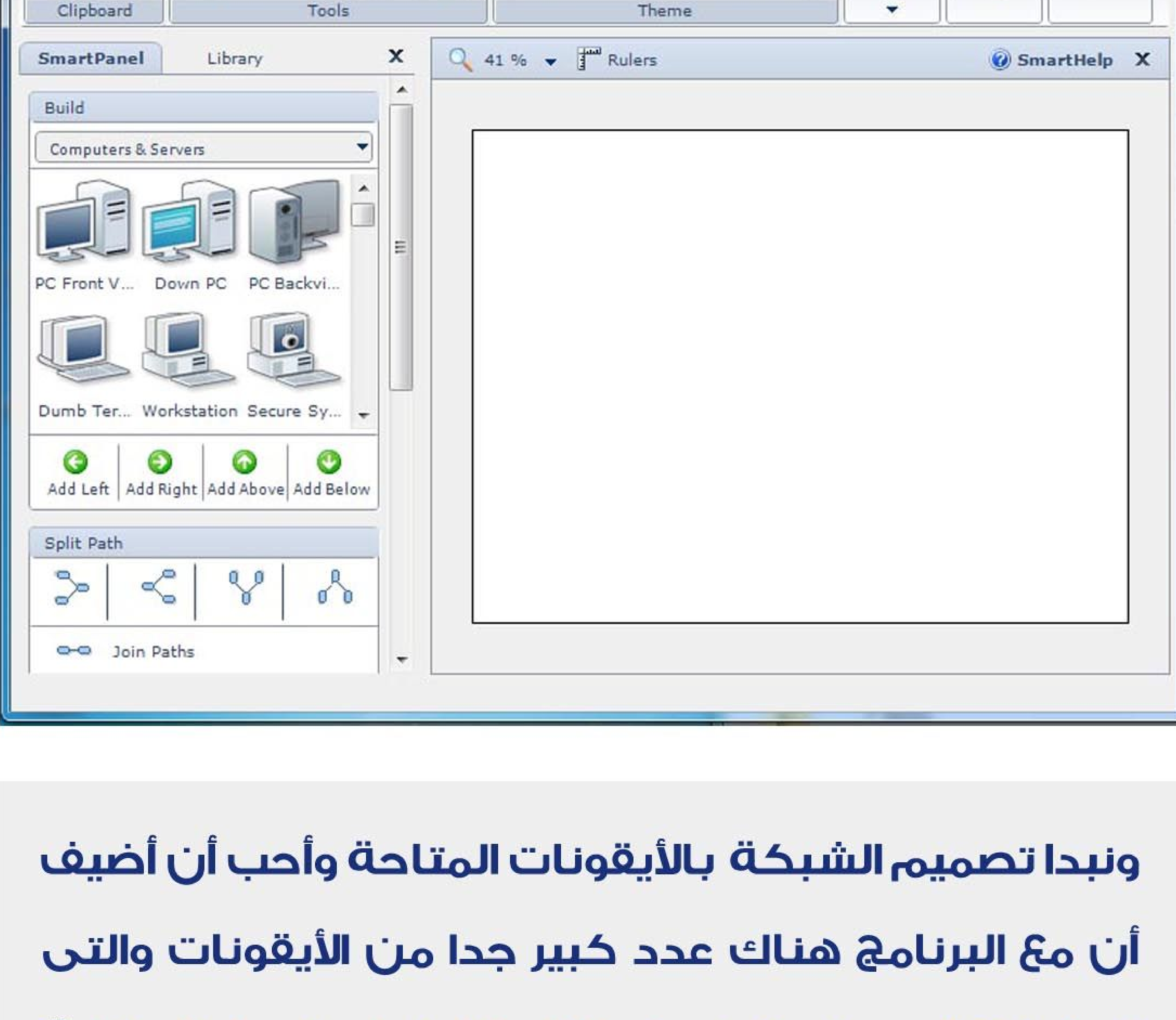




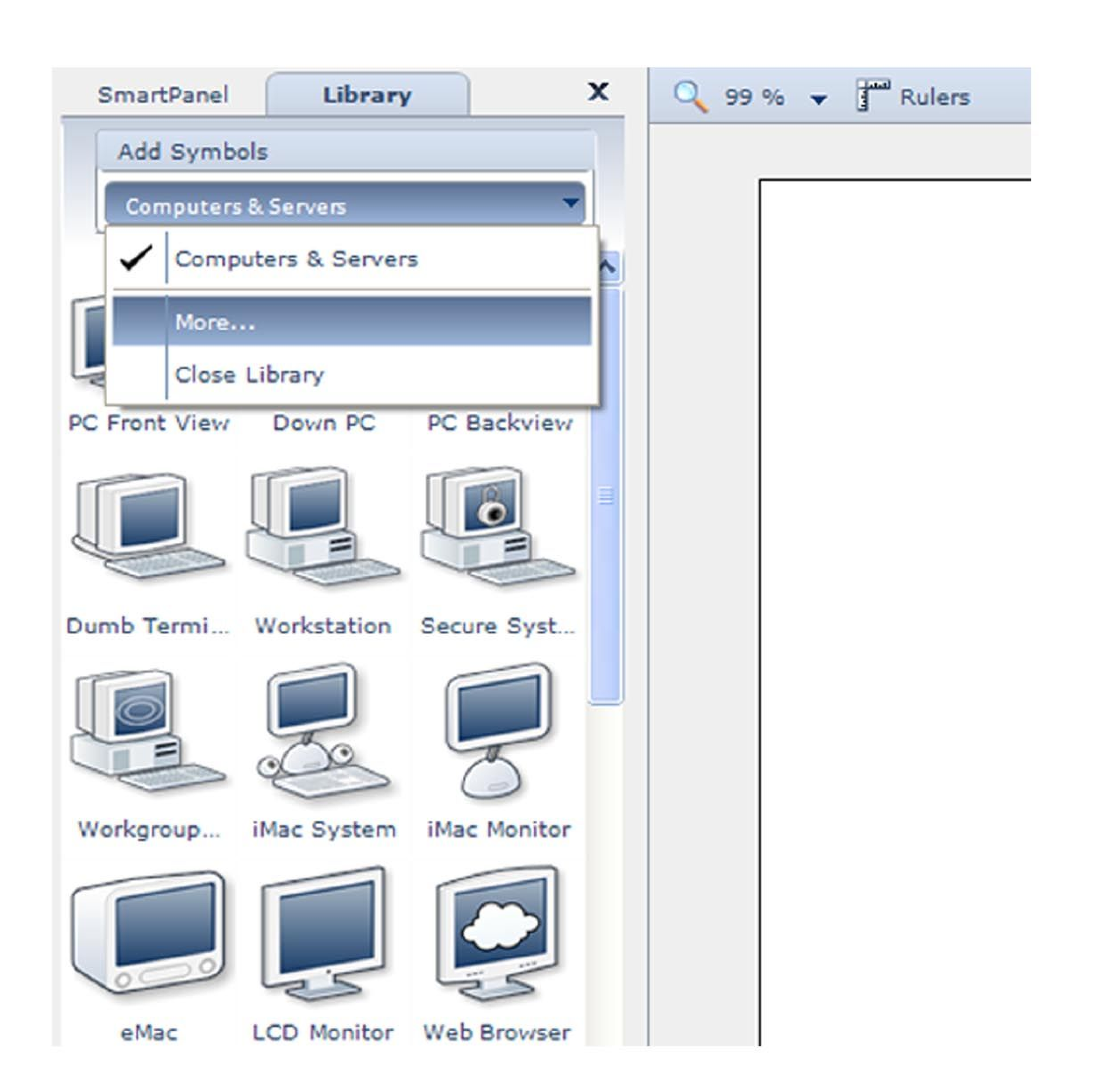




المهم مايلزمنا من كل هذه الخيارات هو الأيقونة المظللة والخاصة بالشبكات نقوم بالضغط عليها لنبدأ رسم المخطط الذي نريده وسوف تصادفنا هذه الصورة



ونبدا تصميم الشبكة بالأيقونات المتاحة وأحب أن أضيف أن مع البرنامج هناك عدد كبير جدا من الأيقونات والتى تستطيع الوصول لها من خلال الضغط على زر المكتبة Library وبعدها تابع معي بالصور

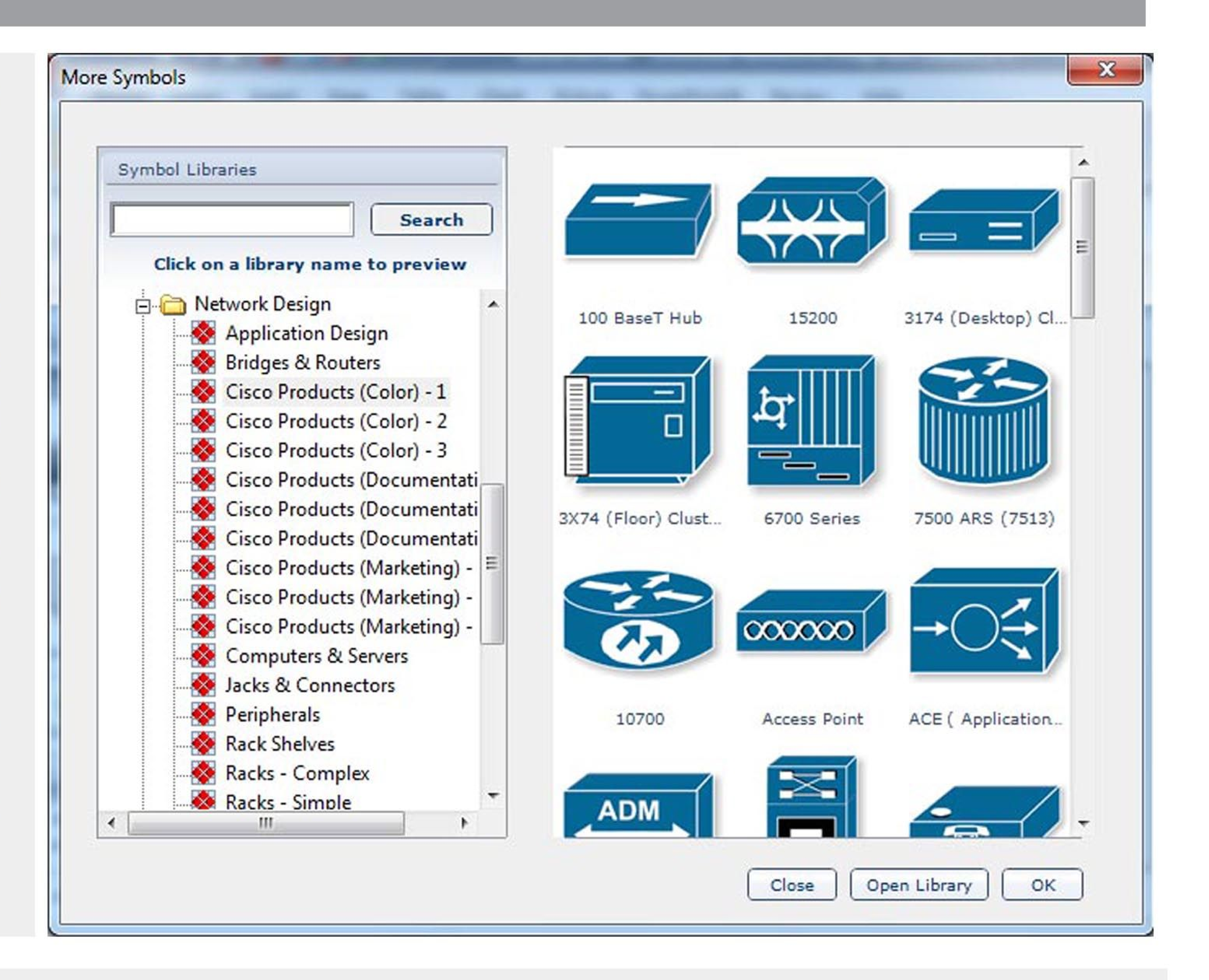


وعندها سوف تتاح لك كمية كبيرة جدا من الأيقونات لرسم المخطط الذي تريده وخصوصا الأيقونات الخاصة بأجهزة سيسكو و يمكنك تجربة البرنامج لسبعة أيام فقط وهذا رابط تحميل البرنامج :

http://download.cnet.com/SmartDraw-20103000/10002466-4_2075-.html

أو من موقع البرنامج الرسمي :

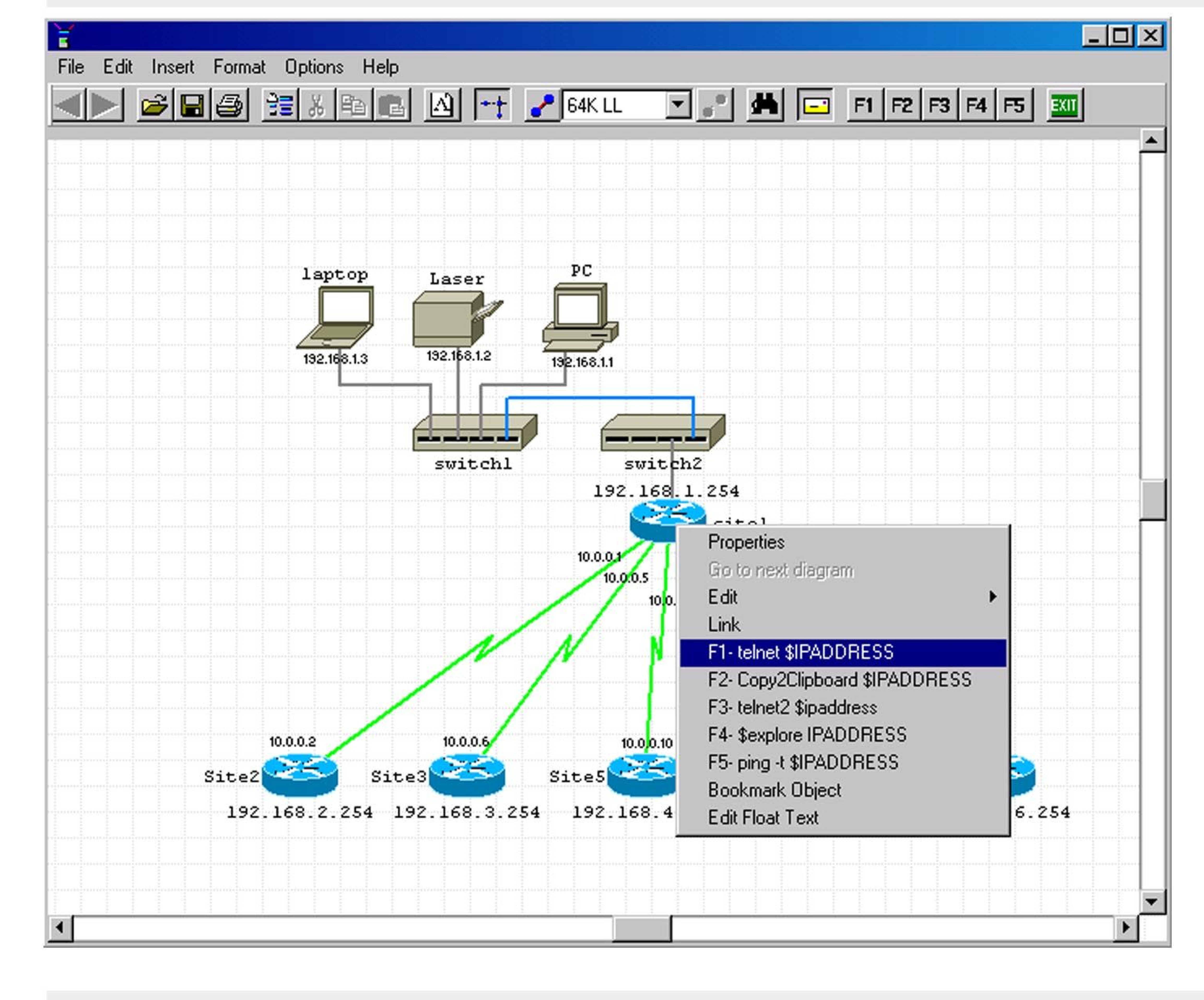
http://www.smartdraw.com/downloads/



البرنامج الثالث

Network Notepad 4.6.6

برنامج بسيط ومجاني ويمكنك ايضا من عمل مخططات للشبكة وهذه صورة توضيحية لكيفية الرسم على البرنامج



لتحميل البرنامج أتجه إلى الرابط التالي

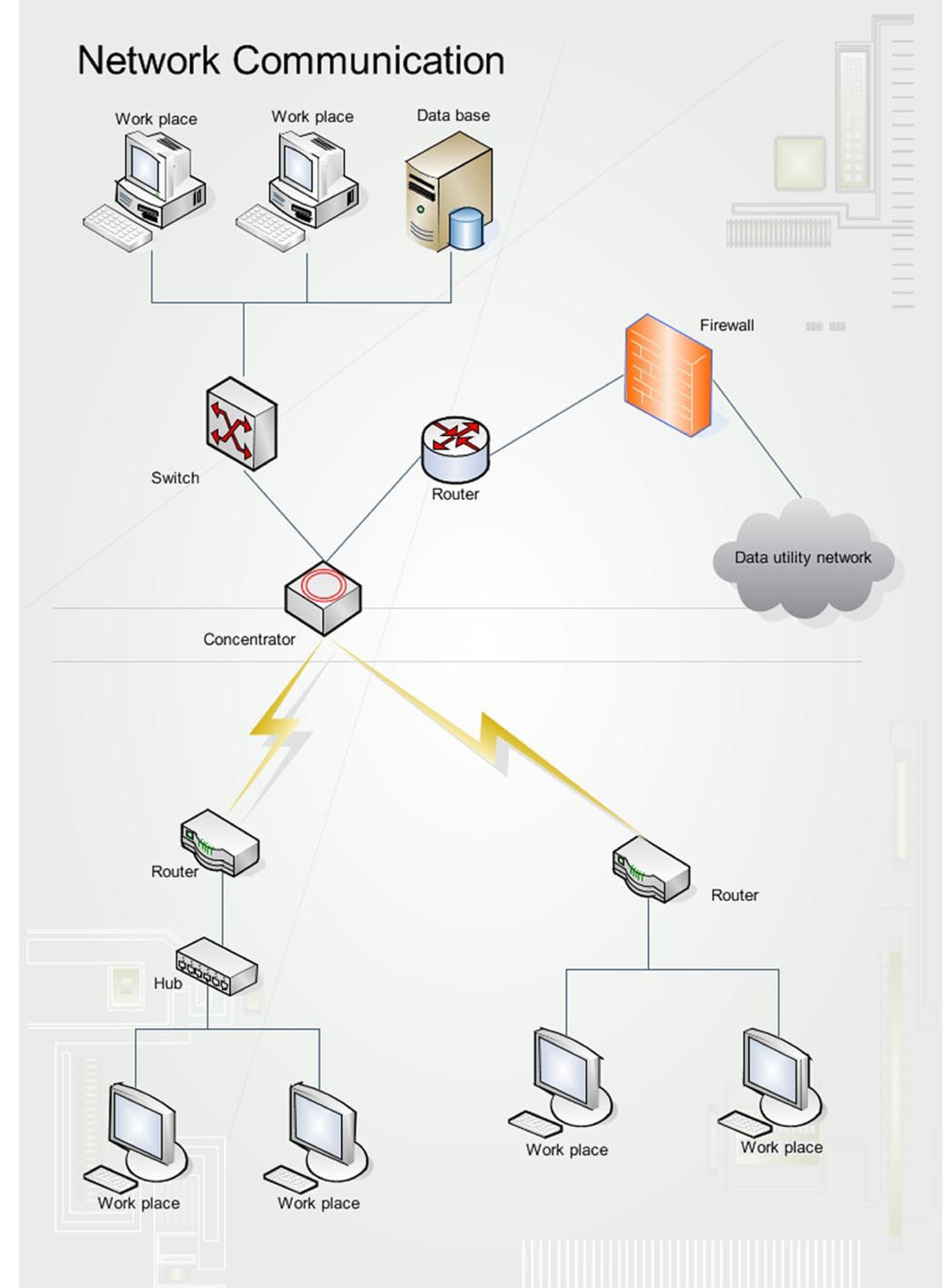
http://www.networknotepad.com/index.htm

لتحميل أيقونات إضافية للبرنامج :

http://www.networknotepad.com/library23.zip

ولتحميل أيقونات خاصة بسيسكو :

http://www.cisco.com/web/about/ac50/ac472/.html



البرنامج الرابع

CuteDraw 2.0

ايضا برنامج بسيط وغير معقد وهو غير مجاني ويقوم بنفس الوظيفة بالنسبة لي لم أقم بتجربة هذا البرنامج هذه صورة توضيحية لكيفية الرسم على البرنامج .

لتحميل البرنامج وتجربته لمدة 30 يوم من موقع البرنامج الرسمي :

http://www.cutedraw.com/download.php

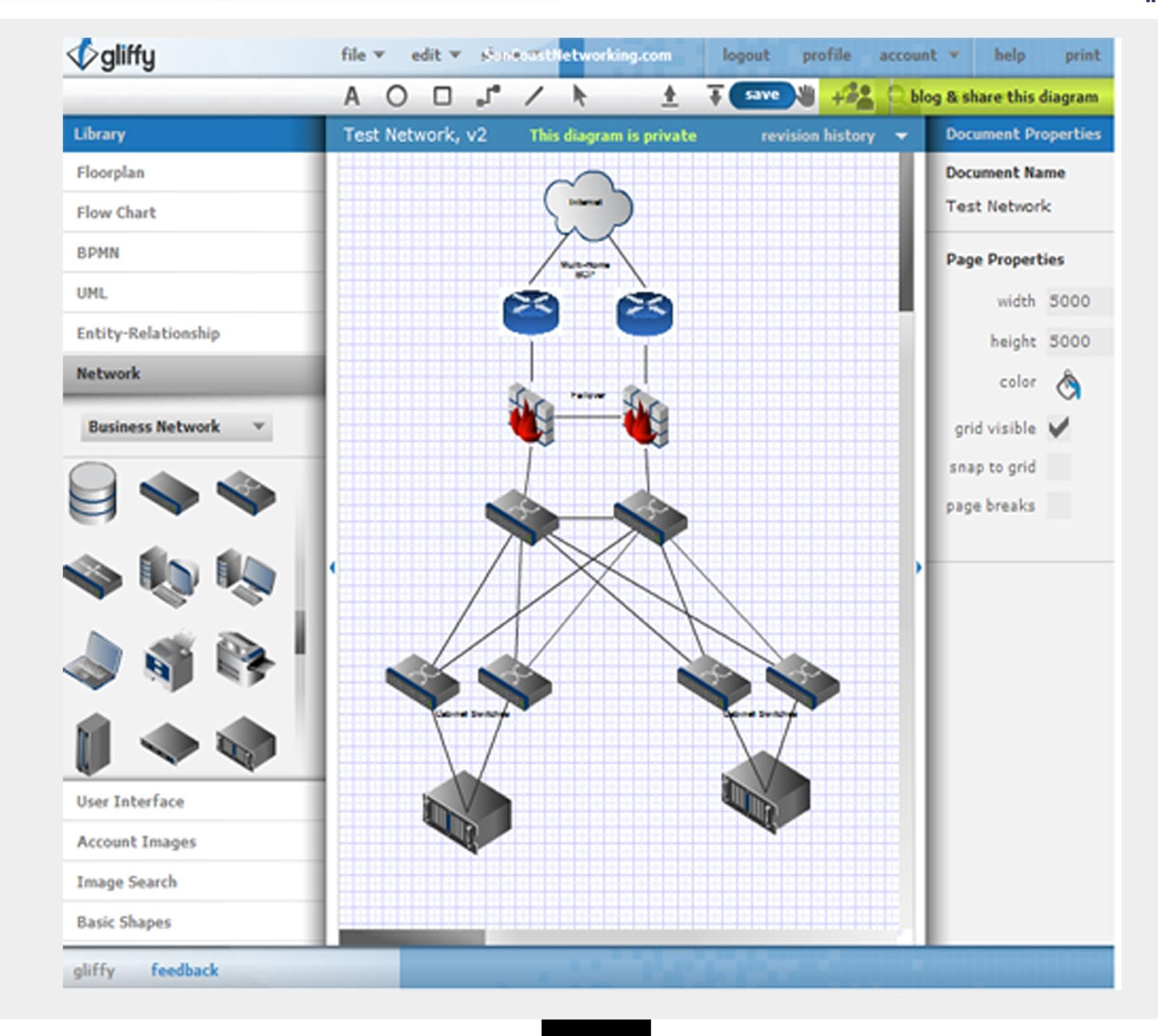
وأخيرا هناك مواقع تتيح لك عمل مخططات on line وبدون الحاجة لتحميل أي برنامج وهي تعمل تحت تقنية الـ Cloud Computing التى سوف تحدث عنها الأستاذ ياسر رمزي في مقال سابق من المجلة .

وهذه بعض المواقع المجانية المخصصة لهذه الوظيفة :

http://draw.labs.autodesk.com/ADDraw/draw.html

/http://www.gliffy.com

وفي الأسفل صورة توضيحية لطريقة عمل مخططات على الموقع الثاني





Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

Whole Technical
One Supplire

Study and implementation of engineering projects

Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942
Website:WWW.EchoTechno.com - E-mail:Info@EchoTechno.com (Soon)

Network Troubleshooting using OSI Model

يعتبر OSI Model بطبقاته السبع نموذج نظري دراسي جميل و مرتب لطريقة عمل الشبكات بكل معداتها و برمجياتها و تقنياتها , و قد مر عليه أي متخصص أو مبتديء في الشبكات و درسه طلاب أقسام الكمبيوتر و الإتصالات في الجامعات

الجديد في الأمر أن يتم استخدام فهمك لهذا النموذج في صيانة الشبكة و تتبع خطائها و وضع حلول لها أو العكس أي أن يكون طريقة صيانتك و تتبع أخطاء شبكتك وسيلة جيدة لفهم هذا النموذج

Group	#	Layer Name	Common Protocols and Technologies	Common Network Components Associated with this Layer
Upper Layers	7	Application	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Network aware applications, Email, Web Browsers and Servers, File Transfer, Name Resolution
	6	Presentation	SSL, Shells and Redirectors, MIME	
	5	Session	NetBIOS, Application Program Interfaces, Remote Procedure Calls	
Lower Layers	4	Transport	TCP and UDP	Video and Voice streaming mechanisms firewall filtering lists
	3	Network	IP, IPv6, IP NAT	IP Addressing, Routing
	2	Data Link	Ethernet Family, WLAN, Wi-Fi, ATM, PPP	Network Interface cards and Drivers, Network Switching, WAN connectivity
	1	Physical	Electrical Signaling, Light Wave Patterns, Radio Wave Patterns	Physical Medium (copper twisted pair, fiber optic cable, wireless transmitters), Hubs and Repeaters

دعنا نتصور هذا النموذج كطبقتين فقط كما تري في الشكل السابق إحداهما عليا وتشمل الثلاث طبقات القريبة في تعاملها مع السوفتوير و الأخري الدنيا و تشمل الأربع طبقات القريبة في تعاملها مع الهاردوير و سنفترض الآن أننا نريد أن نطبق نظرية التعامل بطبقات الشبكة في معرفة سبب انقطاع الإنترنت عن جهاز ما و هي أبسط المشاكل و أكثرها شيوعا و حيث أن المشكلة تخص الإنترنت فسنقوم بتبسيط نموذج OSI الى نموذج TCP/IP و كل ما علينا فعله أن نقوم بضم الثلاث طبقات العليا Application, Presentation, Session, في طبقة واحدة و نتعامل معها على هذا الأساس

و لكل مهندس طريقته في بدء التعامل مع هذا النظام فمنهم من يبدأ من الأعلي و منهم من يبدا بالأسفل و غالبا ما تكون طبيعة المشكلة هي التي تحتم علي مسئول الصيانة من أين يبدأ

و سنقوم في كل طبقة بسؤال أنفسنا بعض الأسئلة منها و أهمها و أكثرها شيوعا هو ما تراه في الشكل التالي ثم نجيب عليها و من ثم نقترح الحل و ذلك في حدود المشكلة التي عرضناها و هي انقطاع الإنترت عن جهاز في شبكة ما

نادر المنسي

Layer 5-7: Upper Layers

هل تستطيع الإتصال بالإنترنت بواسطة المتصفح أو أي برمجيات أخري

Layer 4: Transport

هل لديك جدران نارية Firewall علي جهازك أو تستخدمه في شبكتك

Layer 3: Network

هل تستطيع الإتصال بالراوتر أو gateway الذي يصلك بالإنترنت

Layer 2: Data Link

هل تأكدت من عمل كارت الشبكة NIC علي جهازك

Layer 1: Physical

حاول أن تتأكد من عمل الكابلات التي تصل الأجهزة بالسويتش او السويتش بالراوتر

هيا نبدأ العمل و سنأخذ الطريق من الأسفل الي الأعلي

Layer 1
Troubleshooting

Layer 1: Physical

حاول أن تتأكد من عمل الكابلات التي تصل الأجهزة بالسويتش او السويتش بالراوتر

طبقا لفهمك لهذه الطبقة - و التي يسمونها الفيزيائية طبقا للترجمة الحرفية و أحب أنا أن اسميها الطبقة المادية - فأنت تعلم انها تختص بالهاردوير أي الشيء الملموس من الكمبيوتر أو الشبكة سواء كان ميكانيكيا أو الكترونيا او كهربيا أو معماريا أو بشكل أصح هي الطبقة التي ان حدثت فيها مشكلة فإنك تستطيع تمييزها بالحواس الخمس اي تستطيع أن تراها او تشمها و تلمسها و تشمها بل و تتذوقها أيضا فما بين الملاحظة بالعين عدم وجود فلاش ضوء بعض الأجهزة الي سماع بالأذن اصوات اضطرابات في المراوح و مرورا بالإحساس باللمس بسخونة جزء معين من الهاردوير نهاية الي شم بالأنف شبه اشتعال او احتراق احدي الرقائق الإلكترونية في الجهاز



و تتمثل إحدي مشكلات هذه الطبقة في مشاكل تخص الطاقة الكهربية مثل انفصال الكهرباء خارج الجهاز Device power off أو داخله مثل Power supply أو فشل أحد الشرائح الإلكترونية داخل الجهاز أو بالنسبة لمشكلتنا فإن غالب الأمر أنها تخص كابلات الشبكة فلا تعمل كليا Faulty network cable أو استخدام كابل خاطيء Incorrect cable type

Layer 2
Troubleshooting

Layer 3: Network

هل تستطيع الإتصال بالراوتر أو gateway الذي يصلك بالإنترنت

الجهاز أيضا الي الآن لا يستطيع الإتصال بالإنترنت رغم تغلبنا علي مشكلات الطبقة الأولي و الثانية في هذه الطبقة و التي تسمي بالطبقة الثالة أو طبقة الشبكة Network تقبع عدة بروتوكلات أهمها بروتوكولات التوجيه Routing و بروتوكول IP , و في حال استخدامك راوتر في شبكتك و قمت بإعداده و ضبط بروتوكولات التوجيه به فإنه يجب عليك حينها أن تتأكد من سلامة عمل هذه البروتوكولات و هذه الجزئية فقط هي أحد المحاور الرئيسية في منهج سيسكو الجديد TSHOOT ضمن حزمة CCNP الجديدة أما IP فهو كلمة السر الرئيسية في هذه الطبقة و ما يتعلق به من أقنعة الشبكة و البرتوكولات المساندة مثل DHCP و IP هنا قد يكون عنوان الجهاز الشبكي أو عنوان بوابة الإنترنت gateway أو ربما يكون عنوان DNS IP او عنوان Proxy IP و تكمن المشكلة في عدم قدرة الجهاز من رؤية الأجهزة الأخري في نفس الشبكة رغم اتصالها عمليا و ماديا و تكون عدم القدرة علي الإتصال ناشئة عن عدم وجود هذه العناوين أصلا أو فقدان القدرة علي الإتصال بسيرفر DHCP و الذي يقوم أوتوماتيكيا بحجز هذه العناوين لكل جهاز و لدينا عدة ادوات للكشف عن هذه الأخطاء

ipconfig : يبين إعدادات IP في الجهاز و هنا تتأكد من وجود العناوين الخاصة بالجهاز و سلامة قناع الشبكة subnet mask و كذلك من وجود عنوان بوابة الإنترنت أو الراوتر Gateway

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\nader>ipconfig

Windows IP Configuration


PPP adapter Zain 3G:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.183.137.164
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::952d:cfa0:e2b1:cb5f%11
   IPv4 Address. . . . . . . . . . . : 192.168.190.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.190.1
```

ping : يختبر اتصال الجهاز بعنوان أخر خاصة السيرفر الذي يعطي خـــدمــــات DHCP أو الراوتر

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\nader>ping 192.168.190.3          <----  السيرفر

Pinging 192.168.190.3 with 32 bytes of data:
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.190.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nader>ping 192.168.190.1          <----  الراوتر

Pinging 192.168.190.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.190.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

traceroute : التأكد من سلامة الإتصال بين الجهاز و الجهة التي يريد الإتصال بها و تتبع الخطوات المؤدية لذلك

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\nader>tracert 192.168.190.1          <----  الراوتر

Tracing route to 192.168.190.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.190.1

Trace complete.

C:\Users\nader>tracert 192.168.190.3          <----  السيرفر

Tracing route to LAB2900SRV [192.168.190.3]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  LAB2900SRV [192.168.190.3]

Trace complete.

C:\Users\nader>tracert www.zain.com          <----  موقع ما لنري استجابة الوصول اليه

Tracing route to www.zain.com [72.32.84.240]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4   104 ms   100 ms   119 ms  62.150.83.41
  5   128 ms   119 ms   119 ms  if-10-2.core1.RSD-Riyad.as6453.net [116.0.78.9]

  6   237 ms   229 ms   219 ms  Pos-channel1.mcore3.LDN-London.as6453.net [116.0
.78.42]
  7   227 ms   217 ms     *     Vlan463.icore1.LDN-London.as6453.net [195.219.19
5.38]
  8   207 ms   219 ms   219 ms  xe-10-2-2.edge3.London1.level3.net [4.68.63.105]

  9   248 ms   239 ms   229 ms  ae-34-52.ebr2.London1.Level3.net [4.69.139.97]
 10   293 ms   299 ms   279 ms  ae-41-41.ebr1.NewYork1.Level3.net [4.69.137.66]

 11   277 ms   299 ms   280 ms  ae-61-61.csw1.NewYork1.Level3.net [4.69.134.66]

 12   298 ms   319 ms     *     ae-62-62.ebr2.NewYork1.Level3.net [4.69.148.33]

 13   397 ms   389 ms   389 ms  ae-3-3.ebr2.Dallas1.Level3.net [4.69.137.121]
 14   368 ms   379 ms   389 ms  ae-3-80.edge2.Dallas3.Level3.net [4.69.145.140]

 15   377 ms   389 ms   389 ms  RACKSPACE-M.edge2.Dallas3.Level3.net [4.59.36.50
]
 16   397 ms   389 ms   399 ms  vlan901.core1.dfw1.rackspace.com [72.3.128.21]
 17   377 ms   379 ms   389 ms  aggr4a.dfw1.rackspace.net [72.3.129.15]
 18   347 ms   369 ms   399 ms  72.32.84.240

Trace complete.

C:\Users\nader>_
```

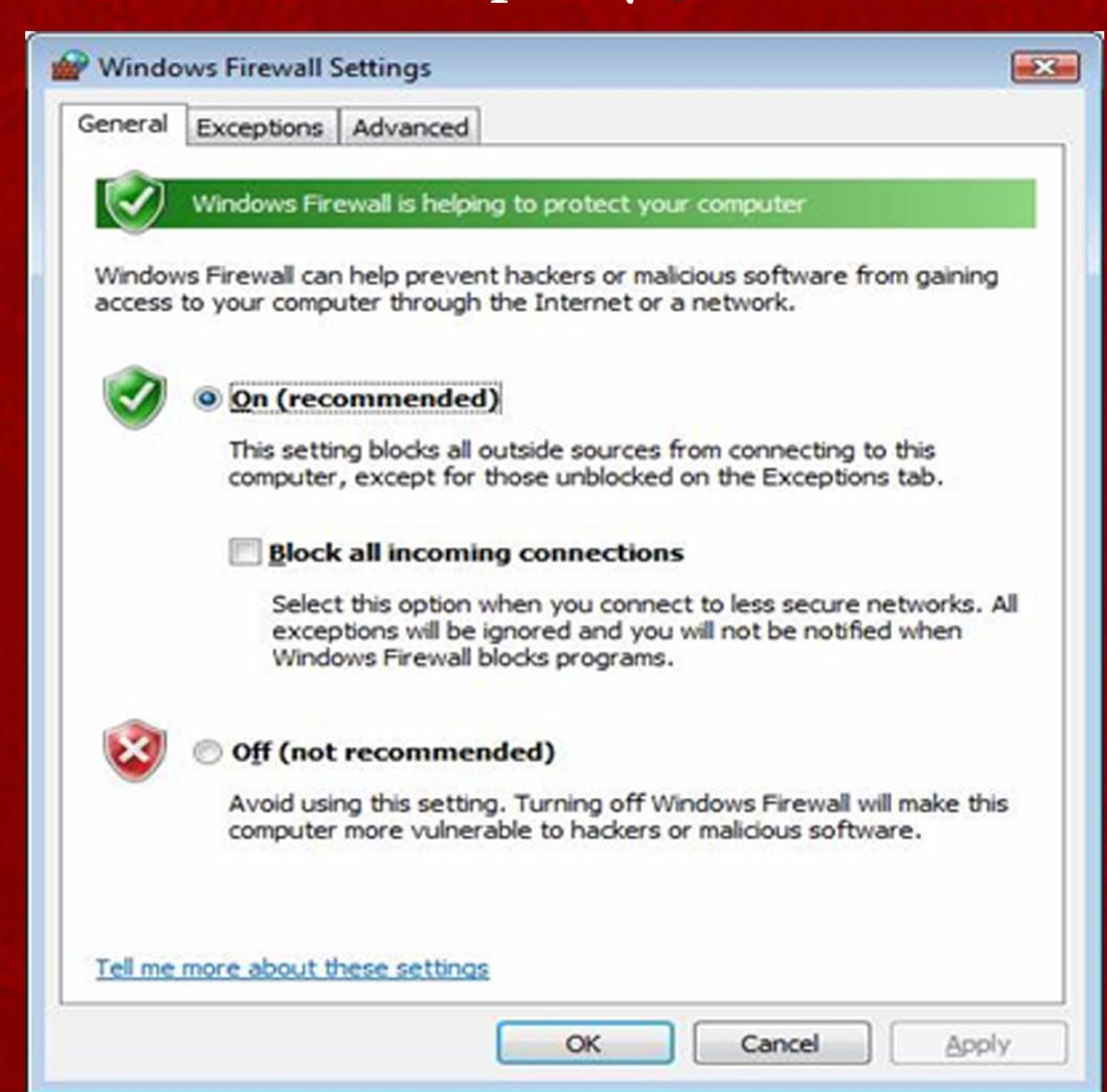
و هناك برمجيات احترافية و متخصصة بل و مجانية أيضا تستخدم أسس هذه الأوامر و لكن بواجهة مرئية مريحة تستطيع البحث عنها علي ألإنترنت

Layer 3
Troubleshooting

Layer 4: Transport

هل لديك جدران نارية Firewall علي جهازك أو تستخدمه في شبكتك

هذه الطبقة و التي تسمي بطبقة النقل Transport layer هي عصب أو قلب نموذج OSI لأنها حقيقة التي تربط بين الطبقات العليا و الدنيا من هذا النموذج و لذلك تختص مشاكلها غالبا في عدم أو صعوبة تدفق البيانات و عمليا لابد أن تتأكد جيدا من سلامة برمجيات أو أجهزة الفايروول لديك و أنها قد تم إعدادها بالشكل الذي تريده و مشكلة إنقطاع الإنترنت بسبب منع الفايرول لتدفق بيانات الإنترنت هي من أكثر مشاكل الإنترنت شيوعا و الفايروول لدينا أما أن تكون شبكية مثل Symantec أو forefront أو محلية مثل برمجيات الفايروول العادية المدمجة في نظم التشغيل أو برمجيات مستقلة مثل Kaspersky او Norton client



و إما أن تكون برمجية مثل ISA و Symantec أو أجهزة مثل PIX و Bluecoat أوراوترات تم إعدادها لتلعب دور الفايروول

Layer 5 through 7
Troubleshooting

Layer 5-7: Upper Layers

هل تستطيع الإتصال بالإنترنت بواسطة المتصفح أو أي برمجيات أخري

في هذه الطبقات و التي أطلقنا عليها اسم الطبقات العليا سنحاول أن نتأكد من عمل البرمجيات التي علي الجهاز فقد يكون كل شيء علي ما يرام من الكابل الي كارت الشبكة و السويتش و مرورا بالراوتر و الفايروول و هنا يجب أن تبحث عن المشكلة الموجودة في برمجيات الإتصال و غالبها تكون بسبب فيروس و انتهاء رخصة برنامج الإتصال أو التصفح أو احتياجه لتحديثات ضرورية او ربما لأنك أخطأت في كتابة اسم الموقع أوما يسمي بمشكلة HTTP قد يكون ايضا نظام التشغيل غير مستقر و يحتاج تحديثات ضرورية أو رقعات أمنية

بعد انتهائك من تتبع هذه الأخطاء فلابد أن تكون نجحت في القدرة علي إعادة الإتصال بالإنترنت

View your basic network information and set up connections

ABCD (This computer) — Multiple networks — Internet

في النهاية اعلم جيدا أنك و أنا معك قد نجد لبس عند محاولتنا للزج بإحدي المشاكل في الجهة أو الطبقة المسؤولة عنها لكن عندما تحدد المشكلة و تحدد الحل فصدقني سيزول هذا اللبس .

و قبل أن أتركك فإنا أعترف أنني لم أقدم لك شيئا جديدا لكن بالتأكيد قدمته لك بطريقة جديدة نوعا ما و أعتقد أنه بواسطة فهم هذا النموذج الفهم الصحيح فإنك تستطيع بإذن الله أن تربط و تجمع شتات كثير من معلومات الشبكات التي تم نثرها في عشرات الشهادات و مئات الكتب و الاف المقالات و ذلك في خطوط عريضة تستطيع أن تجعل من كل واحدة منها كتاب

و لا أدعي أيضا أنك ستكون خبيرا في فهم كل مجالات الشبكات لكن ما أقصده أنك ستستطيع بعد فهم نموذج OSI فهما صحيحا أن تربط ما فهمته حتي الآن في الشبكات بما تريد أن تفهمه و أن تعرف ما موقع ما فهمته في خارطة طريقك للشبكات

أتمنى يوما أن أجد كتاب عربي كامل عن هذا النموذج يشرح كل ما فيه بشكل تتعانق فيه السطور النظرية مع التطبيقات العملية ليكون كل ما نعرفه في الشبكات مرتبا طبقا للطبقات و ليس طبقا للشهادات المعروفة ليكون مرجعا لأي من يريد أن يلج عالم الشبكات من أوسع أبوابه

أساسيات التعامل مع الـ

intrusion detection and prevention systems

شريف مجدي

فى هذا المقال سأتكلم عن موضوع مهم فى عالم ال security و هو اساسيات التعامل مع اجهزة منع و كشف المتطفلين فى الشبكه (sensors) و الذى يساعد على بقاء الشبكه امنه من الهجمات الخارجيه

قبل ان ابدأ احب ان اوضح بعض المصطلحات سريعا :

IPS : هو عباره عن جهاز يقوم بتحديد الهجمات و التصدى لها وامكانيه تعديلها و تسجيلها لهذا فيجب ان يكون فى مسار البيانات

IDS : بعكس الاول تماما فهو قادر فقط على تحديد الهجمات و ارسال تحذير الى management workstation

in-line mode : هى الوضعية المثلى لجهاز ال IPS و فى هذه الوضعية يكون الجهاز فى مسار تدفق البيانات اي ان البيانات يجب ان تمر من خلاله.

promiscuous mode هو الوضع الخاص باجهزه ال IDS ويتم توصيل الجهاز الى span port or Remote span الى ال switch ليستطيع الجهاز ان يقوم بعمل فحص للبيانات التى تمر اليه و ليس من خلاله مثل الحاله السابقه , و ايضا من الممكن ان يستعمل ال IPS هذا الوضع

اليه عمل هذا الجهاز و طرق تعرفه على الهجمات :

يعتمد هذا الجهاز على اكثر من طريقة و سنتعرف على اهمها فى هذا المقال

1- signature-based

2- policy-based

3 anomaly detection

الطريقة الاولى تعتبر الطريقة الاساسية التى يتم الاعتماد عليها و هى تقوم بتحديد الهجمات الشائعه (common attack) , وتعتمد على عمل signature لكل هجمه

مثال 1 : هناك هجوم يستهدف ال http server و بعد تحليل هذا الهجوم من قبل الخبراء وجدوا الاتى .

حتى يستطيع المهاجم اتمام هذا الهجوم يجب ان يرسل packet لها هذه الصفات تحوى على هذه ال string "10\.1\.1\.100"" .

هنا يتم تصميم signature لهذا الهجوم و فى هذه الحالة نصمم هذه ال sig بحيث تقوم بالبحث داخل ال packet عن ال string السابق و يقوم ال IPS بتمرير جميع الترافيك على هذه ال sig لتقوم بفحصه و تتاكد من انه خالى من هذا الكود الخبيث الذى فى هذه الحاله هو 10\.1\.1\.100 , هذا مثال بسيط لتوضيح الامر فقط فهناك هجمات شديده التعقيد و ال sig التى تقوم بالتصدى لها اكثر تعقيدا

الان نفترض ان هناك هجوم و يقوم ال IPS بعرض هذا الهجوم على كل sig. و جاء دور ال sig. المخصصة لكشف هذا الهجوم ماذا سيحدث ؟

سيحدث ما يسمى بال sig triggering اى تم التحقق من ان هناك هجوم جارى و هنا تقوم ال sig بعمل عده اشياء

1 سريعا سيقوم بارسال alert و تخزينه فى ال event store حيث يستطيع مراقب الشبكه ان يعرف ان هناك هجوم جارى

2 تقوم باتخاذ قرار حسب طريقة اعداد ال sig فمثلا عندما يتم تصميم ال sig يجب ان تحدد ماذا يفعل هذا الجهاز اذا حدث الهجوم



• هل يقوم بارسال alert فقط ؟

• هل يقوم بمنع ال packet التى تحتوى على هذا الهجوم فقط ؟ (طبعا لا اريد ان اهين ذكاء القارىء و اقول ان هذا فى حاله ال in-line mode اى يجب ان يكون الجهاز IPS)

• هل يقوم بمنع المهاجم منعا كاملا ؟

• هل يقوم بارسال RST لقطع الاتصال

• هل يقوم بعمل log للهجوم (اقصد هنا عمل capture له و من ثم عرضه عن طريق wireshark مثلا)

و خيارات اخرى كثيره وذلك حسب الحاجه فهناك هجمات ليست خطيره يكفى ارسال alert و هجمات اخرى خطيرة فيجب فى هذه الحاله اتخاذ اكثر من قرار , منع الهجوم و المهاجم

انواع ال sig :

1 - builtin sig.

2 - tuned sig.

3- customized sig.

النوع الاول هو الشكل الاساسى لكل sig من دون تغير اى اعدادات او تغير شىء بها , و ياتى الجهاز بحوالى 2000 sig لتحديد معظم الهجمات الشائعه و جميعها تم تصميمه من قبل سيسكو

مثال 2 : عندنا شبكة تحتوى على عده سيرفرات ftp و فى نفس الوقت هناك هجوم منتشر يستهدف ال ftp server و هذا الهجوم مازال فى 0 day و لم يتم اصدار اى sig له من سيسكو

الان ماذا نفعل هل نترك الشبكه مهدده حتى يتم اصدار ال sig ؟ طبعا لا , سنقوم بعملها بنفسنا , اولا نبحث و نقرأ كثيرا بخصوص هذا هجوم و بعد البحث و جدنا ان هذا الهجوم يميزة هذه الكلمة "FtP AtTAcK"

الان نقوم بتصميم sig بسيطة جدا تقوم بالبحث عن هذه الكلمة و منع ال packet و اجراء اى action من الذين تم ذكرهم سابقا لمنع هذا الهجوم مؤقتا لحين نزول sig من قب سيسكو

signature engines :

بعد ان علمنا ان ان هناك عدد كبير من ال sig لابد من تنظيم هذا العدد بطريقة معينة حتى لا يحدث اى تاخير ينتج من فحص الترافيك و هنا تم تقسيم ال sig الى مجموعات متعدده , كل مجموعه تسمى engine و تحتوى هجمات تستهدف هدف معين فمثلا تم تجميع الهجمات التى تهدد ال http ووضعهم فى engine واحد , و يتم تشغيل الجهاز يتم تحميل كل engine فى ال ram كى يستطيع الجهاز تمرير الترافيك اليها

ويكون ذلك in-parallel و ليس ان in-serial اى سيتم عرض ال packet على جميع ال sig فى ال engine الواحده فى وقت واحد .

وهذه بعض ال engine

ATOMIC Signature Engines :تهتم هذه المجموعه من ال sig بالهجمات التى تتم عن طريق packet منفرده

FLOOD Signature Engines : هجوم ال DOS & DDOS

SERVICE Signature Engines : بعض الخدمات المختلفة و البرتوكالات العامة

STRING Signature Engines : تقوم بعمل match ل string معينه عن طريق regular expression

SWEEP Signature Engines: تقوم بتحديد مايسمى بال fingerprint

TROJAN Signature Engines : تكشف التروجان

TRAFFIC Signature Engines : بعض البروتكولات

AIC Signature Engines : مخصصه لل deep inspection for HTTP and FTP only

STATE Signature Engine : نوع مخصص لل state protocols

META Signature Engine : اما هذا فيقوم بكشف الهجوم الذى يسبقة عدة هجومات اخرى مثل NIMDA attack

NORMALIZER Engine : خاص بال anomaly detection

نعود الى ال alerts مرة اخرى و كما قلنا يقو م ال IPS بوضع هذه ال alert فى ال event store عند حدوث هجوم

واريد هنا ان قوم بشرح مصطلح بسيط هو alert severity و اذا ترجمنا هذه الكلمة نجد المعنى هو شده الانذار بمعنى اخر ما هو مستوى الهجوم الذى سبب هذا الانذار , و هذه هى المستويات

low – medium – high – informational

ويمكنك ان تقوم بتغير ال default لكل sig حيث تقوم بعمل alert بالمستوى الذى تراه انت مناسب و من الممكن تركه كما هو على حسب وجه نظر سيسكو , فى بعض الاحيان يجب تغيره

positive and negative alerts :

ناتى هنا الى مصطلحان جديدان و هو ال false positive and negative alarms فإذا كان المخترق بارع من الممكن ان يقوم بخداع ال sig و يتجنب الكشف و يستطيع تمرير الترافيك الخبيث الى داخل الشبكة و هنا نطلق هذا المصطلح false negative

مثال 3 : اريد ان اقوم ببدء هجوم على شبكة محميه عن طريق IPS device و بعد البحث وجدت ان هناك sig ستقوم بكشف هذا الهجوم لنقل مثلا لان الهجوم يميزة هذه الكلمة "ATTack"

عندها اقوم انا بعمل مراوغه بسيط و اخدع الجهاز و تغير هذه الكلمة الى تميز الهجوم الى "attACK" عندها سيتم الهجوم, و لكن خداع ال IPS يحتاج الى مخترق بارع .

اما ال false positive فهو عندما يرى ال IPS ترافيك سليمة و غير خطيرة و يعتقد انها هجوم و يقوم بمنعها . والسبب فى ال false positive & false negative هو التصميم السىء لل signature .هذا بالنسبه لل signature-based , أما النوعان الاخران

Policy-Based :

تعتمد هذه الطريقة على أولويات الشبكة و الترافيك المسموح له بالمرور فى الشبكه فمثلا اذا كان هناك مجموعه سيرفرات http فيمكن ان نتبع سياسه تمنع مرور اى نوع اخر من الترافيك مثل ال ftp مثلا, ففى هذه الحاله نقوم بعمل policy تمنع اى ترافيك من المرور سواء كانت خطيرة ام لا و ارسال alert الى ال event store و السماح فقط لل HTTP

Anomaly-detection :

هذه الطريقة جديده على cisco sensors و تم تصميمها لتعمل جنبا الى جنب مع ال signature-based method

وهدف الرئيسى منها هو منع انتشار ال worms فى الشبكه , فيتم اتباع طريقة معينه لمعرفه ال normal traffic و ارسال alert فى حاله اى تغيير عن normal الذى تم التعارف عليه

(POSFP (passive operating system fingerprint

هى تقنيه جديده فى ال IPS V.6 تقوم بالتعرف على نظام التشغيل للضحيه

مثال 5 : قام ال IPS بالتعرف على هجوم على linux server يملك هذا ال 10.10.10.10 ip عندها يقوم ال IPS بالبحث فى قاعده بيانات يمتلكها ليتعرف على نوع نظام التشغيل الخاص بالضحيه .

فى هذه الحاله سيجده مثلا linux RedHAt ووجد ايضا ان هذا الهجوم يستهدف ال ISA server و لن يسبب اى ضرر للينكس عندها يعرف انه ليس من الضرورى ان يقوم باراسال alert وذلك تقليلا من عدد الانذارات لسهوله التحقيق فيهم فيما بعد , او من الممكن ان يرسل alert ولكن سيكتب بها "not relevant"

اخيرا احب ان اتكلم عن best IPS location

يعتمد هذا الموضوع حسب ظروف الشبكة التى تريد حمايتها و لكن الشائع هو خلف الراوتر او الفايرول ولكن هذا لا يمنع انه فى بعض الحالات يمكن وضعه امام ال firewall

الموضوع مازال اكبر من ذلك و ان شاء الله نتكلم عن خواص اخرى فى هذا الجهاز الرائع

خلق
علم
عمل

أنس الأحمد

بسم الله الرحمن الرحيم

اعذروني إخوتي جميعاً إذا كانت مقالاتي مملة بعض الشئ ولا تدخل كثيراً في صلب اختصاص المجلة ولكنني أظن أن جانباً كهذا الجانب لوبقي في مجلتنا فمن الممكن أن يساهم نوعاً ما بتأكيد رسالة المجلة التي تريد أن توصلها ألا وهي الخير ثم الخير ثم الخير للجميع .

وانطلاقاً من هذه النقطة وتكملة لمقالة العدد السابق التي أكدت على ضرورة اقتران العلم بالعمل أود أن أؤكد على عامل يتكامل مع العاملين السابقين ولا نستطيع عزله عنهما .

حين نتحدث عن مفهوم الأخلاق قد يخيل للبعض أنها إحدى قصص شهرزاد القديمة التي انقرضت أو المدينة الفاضلة التي لم تتجاوز أسوارها حدود ورق الفلاسفة وكتاباتهم وأن عصرنا المادي الحالي يعترف بمقدار الإنجازات والمكاسب التي يحققها الإنسان بغض النظر عن الطريقة أو الأسلوب وبتجاهل مقدار الضرر الذي سببه لمن حوله .

أخوتي في الله قد يتراءى لنا من خلال مراقبتنا لمن حولنا أن كلام هؤلاء يعتريه شئ من الصحة ولكن صدقوني أن ذلك مجرد أوهام فالإنجازات لاتقاس بالماديات فقط ولا أقصد بكلامي هذا ترك الإنجازات العملية ولكن فقط القيام بعملية اقتران بسيطة بين الأخلاق وكل ما ننجزه في حياتنا فذلك يسهم في زيادة محبة الله والناس لنا ولإنجازاتنا وبالتالي إضفاء المزيد من النجاح والاستمرارية .

وحين نعود إلى أساسيات ديننا الحنيف لوجدنا أن الأخلاق مقدمة حتى على العبادات الأساسية ففي حديث رسول الله صلى الله عليه وسلم بما معناه عن المفلس الذي يأتي يوم القيامة بصوم وصلاة ويأتي وقد شتم هذا وقذف هذا وأكل مال هذا فتؤخذ من حسناته وتعطى لهم ثم تؤخذ من سيئاتهم وتطرح عليه ثم يطرح بالنار وكذلك قوله تعالى حين يبين صفات عباد الحمن التقاة بعد بسم الله الرحمن الرحيم (وعباد الرحمن الذين يسيرون على الأرض هونا وإذا خاطبهم الجاهلون قالو سلاما والذين يبيتون لربهم سجداً وقياما)

ونلاحظ أن التعفف عن الجاهلين وهو خلق سبق الصلاة وقيام الليل وهو عبادة

كذلك يجب ألا نكتفي بمجرد الفخر بما أننا أصحاب حضارة وإنجازات يعترف بها العالم إلى اليوم فحضارة أجدادنا استمرت بأخلاقهم وحتى إنجازاتهم العلمية ازدهرت في وقت رفع فيه لواء الأخلاق .

طبعا هذه دعوة لدمج الأخلاق في كل نواحي حياتنا بما فيه العلم والعمل لأن ذلك يعني الأمانة في منح ما نملكه من معلومة أو مجهود وهذا يعود بالنفع على الجميع

أرجو من الله أن يلهمنا جميعاً صلاحاً وتقوى في الدنيا والآخرة ويمدنا بالقوة لفعل الخير ونشره

نـــادر
المنسي

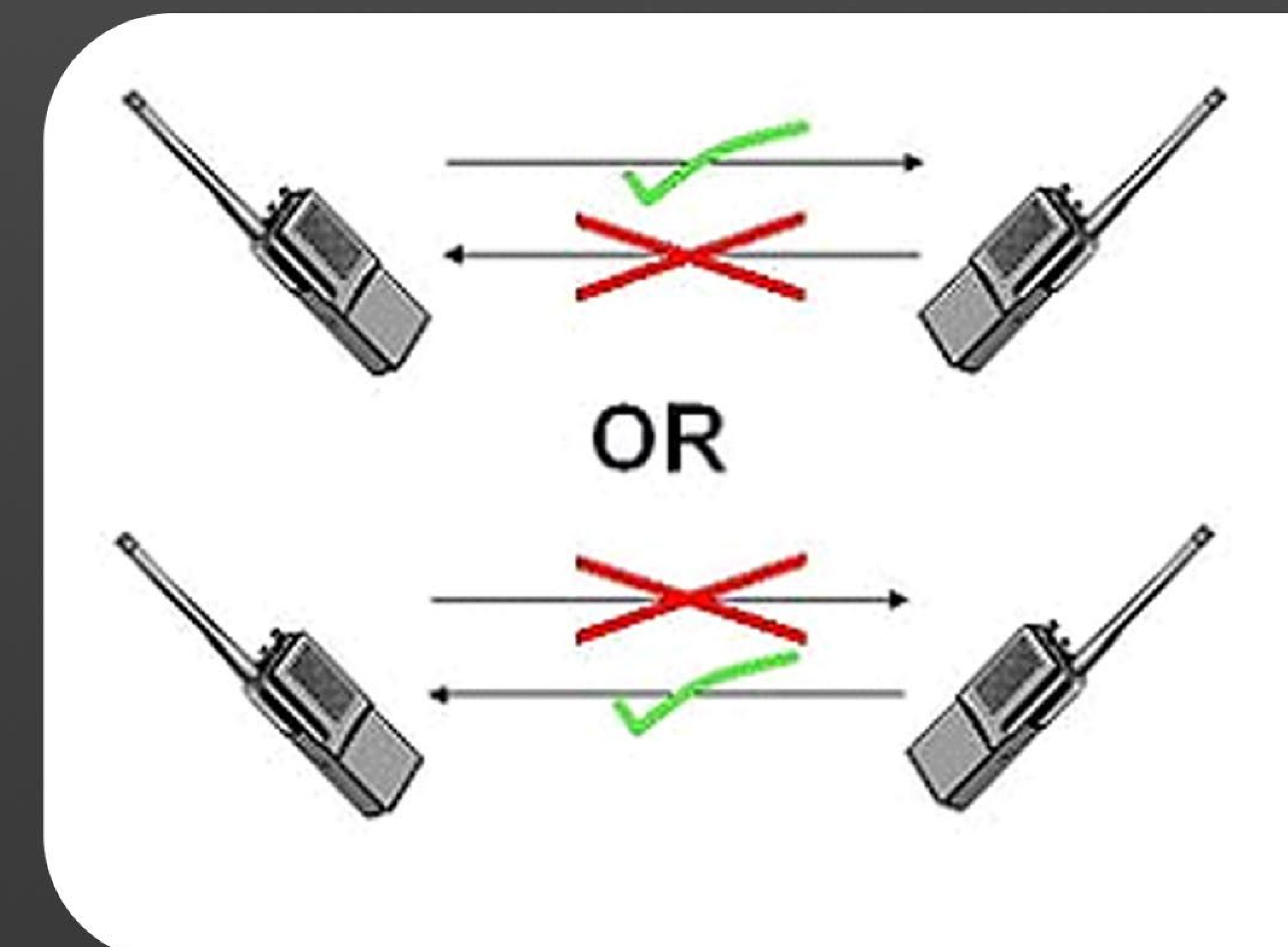
الإرسال والإستقبال من خلال الكابـــل

عندما كنت أستقل القطار من محطة بنها الي محطة منوف حيث توجد كليتي كان القطار ينتظر احيانا في محطة الباجور كي ينتظر القطار المقابل لأن شريط القطار فردي لا يتحمل قطارين في نفس الوقت ودعنا نسمي تلك الطريقة half duplex

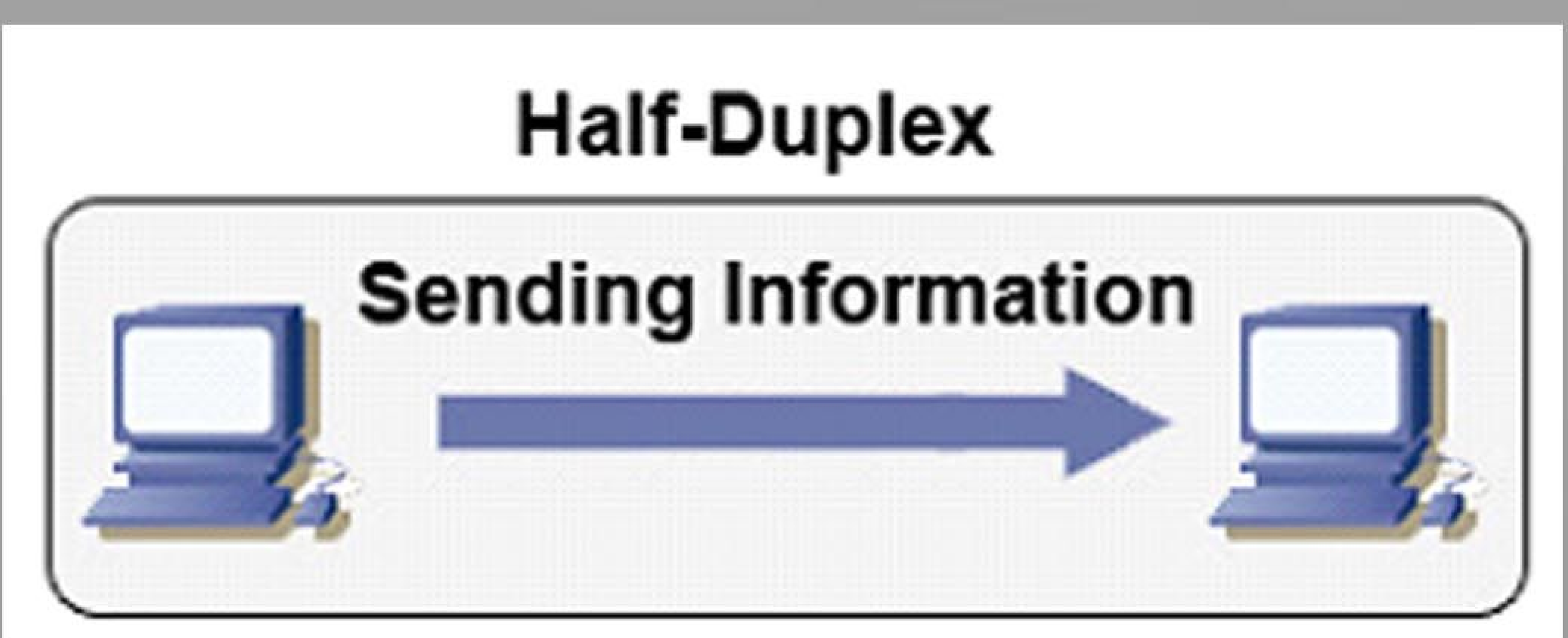
وعلي العكس فإن المسافة ما بين محطة بنها الي الزقازيق كان شريط القطار مزدوج يسمح لقطارين متقابلين بالمرور وسنسمي تلك الطريقة full duplex

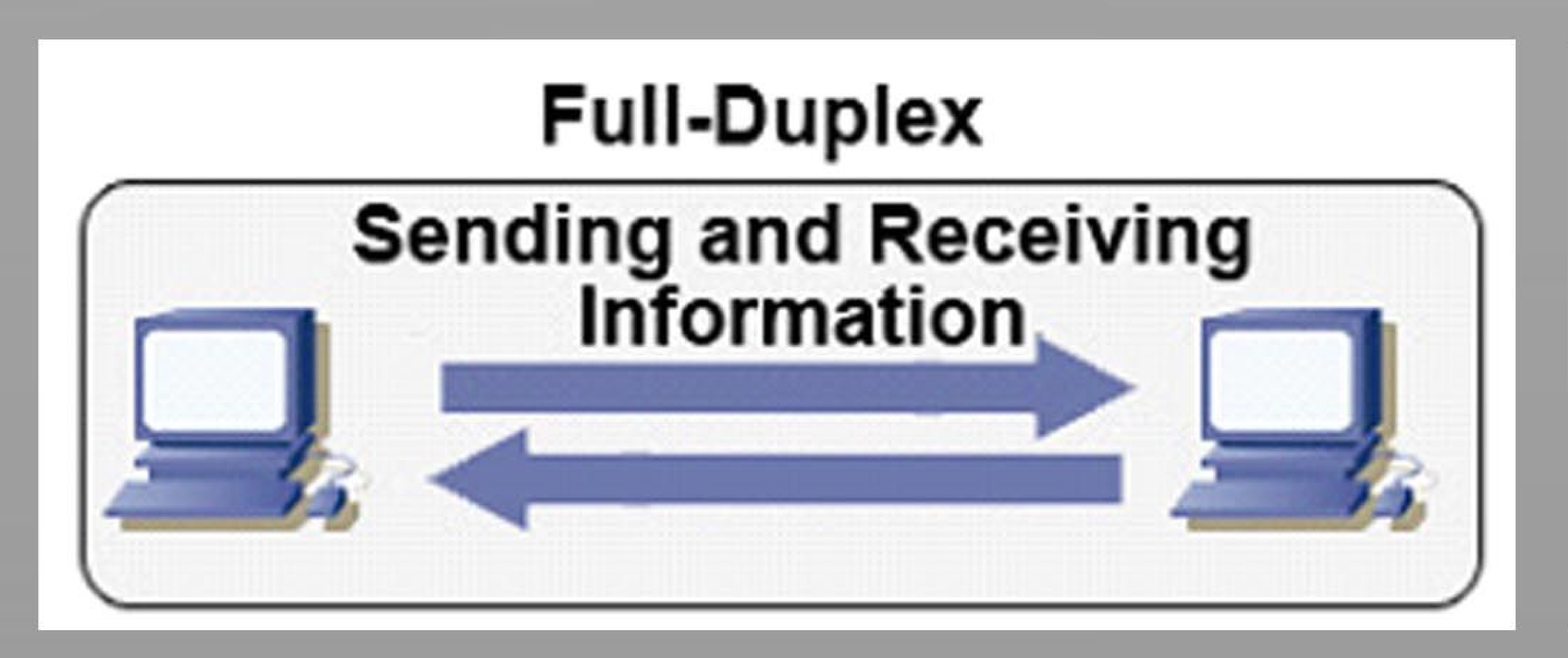
هذه هي فكرة ارسال و استقبال الإشارات من خلال الكابلات و مدي تطورها علي مدي الزمن

حيث انhalf duplex هي نقل الإشارة ايابا فقط او ذهابا فقط ولا يمكن الإرسال وا لإستقبال في نفس الوقت مثل أجهزة الشرطة اللاسلكية حتي انك تسمع كلمة ''حول'' بعد انهاء كل فقرة ليخبر الطرف الأخر انه انهي حديثه والمسار فارغ.

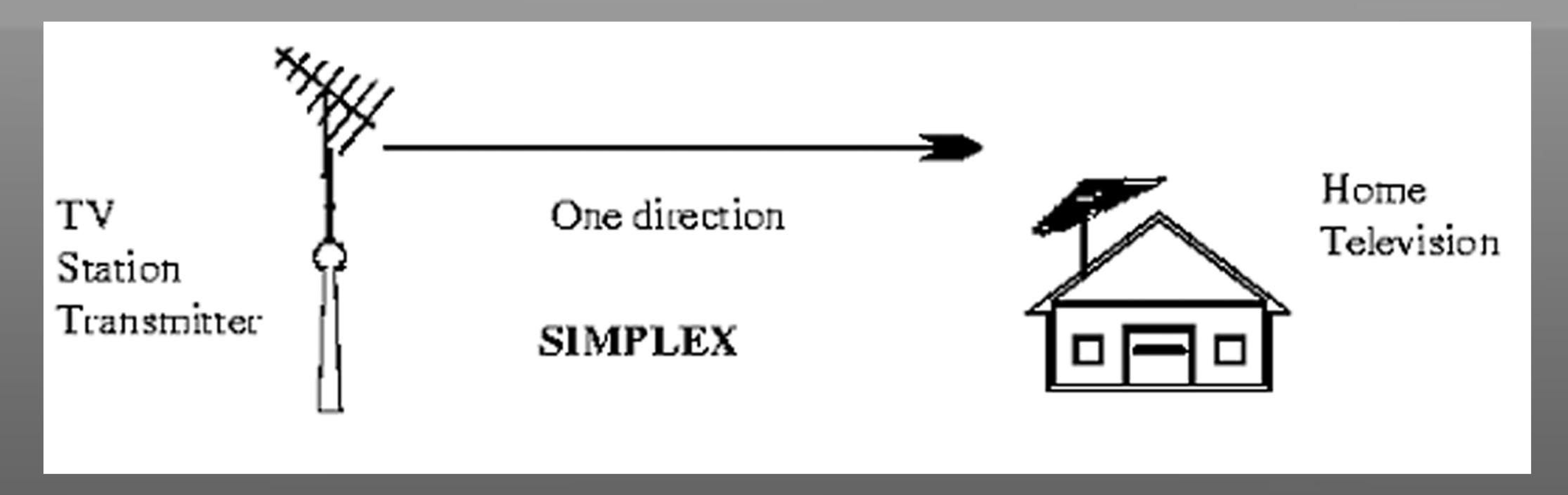


full duplex وهي تسمح بنقل الإشارة ذهابا و ايابا في نفس الوقت اي ترسل وتستقبل مثل جميع انظمة الإتصال التي تستطيع ان تتحدث وتسمع في نفس الوقت والتى تشمل أيضا منظومات شبكات الحاسوب .





واضافة لذلك فإنه يوجد نظام يدعي simplex يسمح فقط بالإرسال من جهة لأخري ولا يسمح اطلاقا بالعكس مثل الإرسال التلفيزيوني واتصال الطابعات بالحاسوب



ولارسال اشارة داخل الكابل بمدي ترددي اعلي من نطاق الكابل

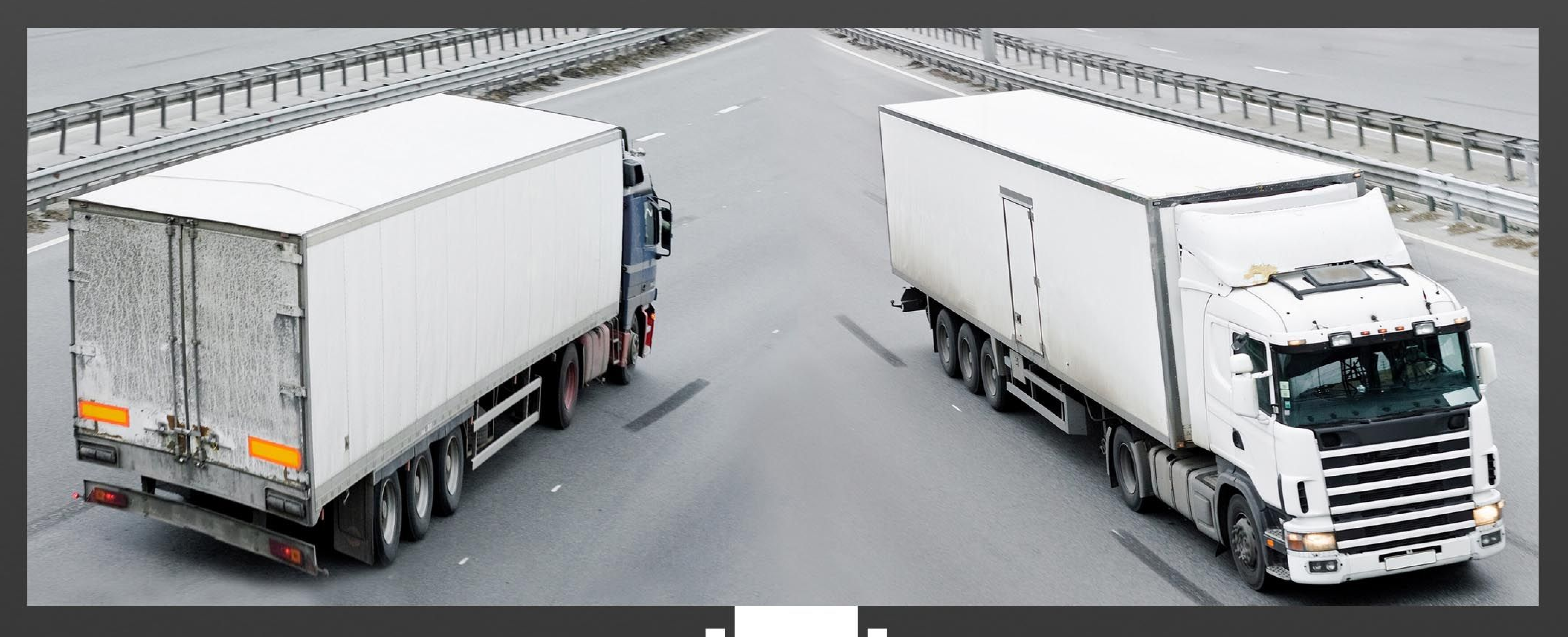
في الشبكات المحلية فإنه يتم استخدام زوجين من كل اربع ازواج للإرسال والإستقبال زوج يرسل والأخر يستقبل

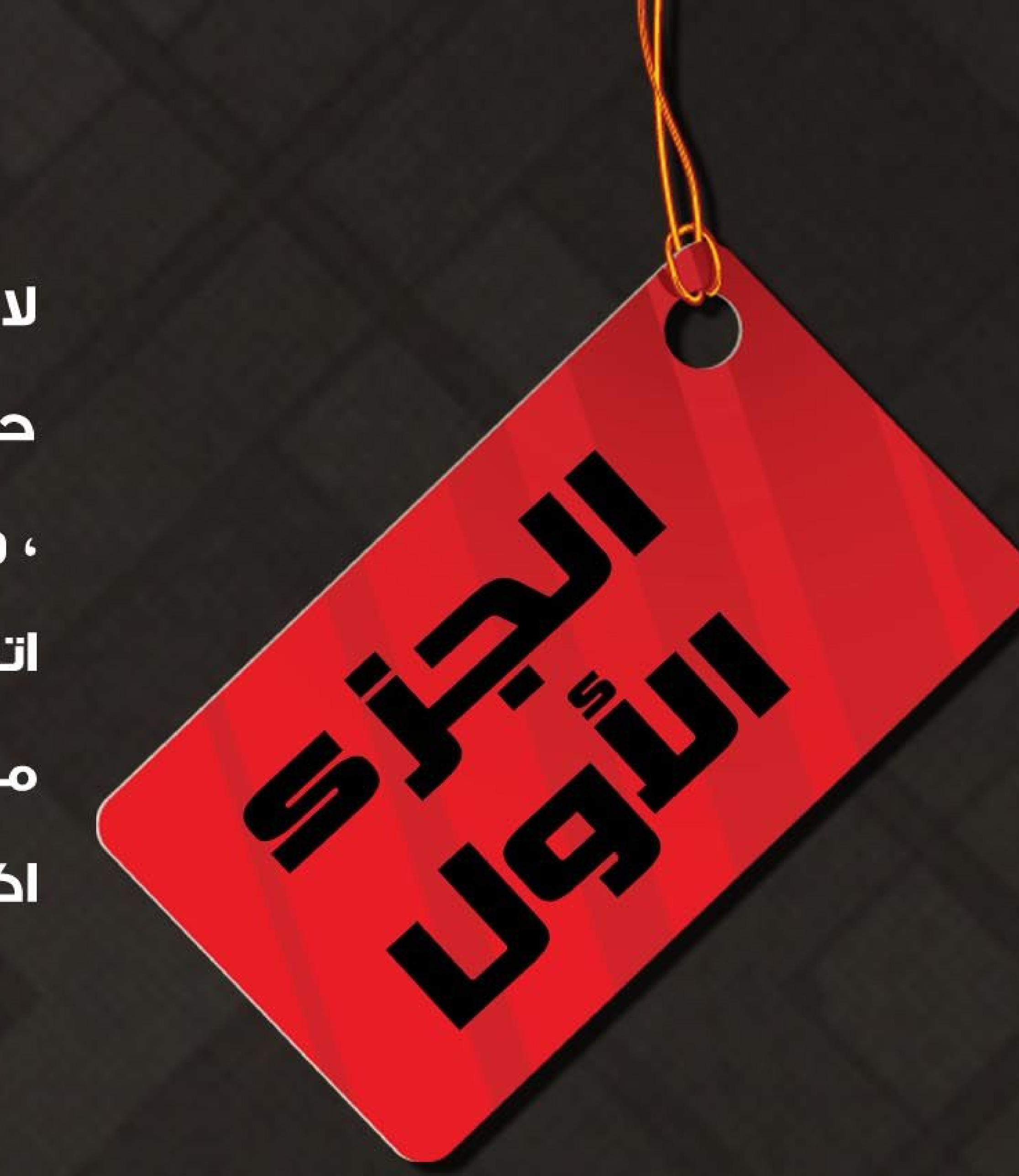
ومن الممكن ان تعتبر المسار مثل طريق السيارات تسير فيه سيارة واحدة فقط كل فترة زمنية خلال مسافة من الممكن ان نستغل تلك الترة الزمنية ونجعل ثلاث سيارت مثلا تسير في نفس المسافة في نفس الزمن اي ثلاث سيارت كل ثانية بدلا من واحدة كل ثانية

ولكن قطعا سيأتي يوما وتزداد السيارات عنا لابد من عمل طرق اخري اي ننشيء مسارين اضافيين احدهما ايابا والأخر ذهابا

ولكن الا تلاحظ احيانا انه في اوقات الذروة تجد ان احد جانبي الطريق مشغول والأخر المقابل فارغ .. فلم لا نستغل هذا الفارغ

وهذه هي فكرة جيجا ايثرنت وهو استخدام كافة المسارات ذهابا وايابا لإرسال واستقبال الإشارات وهي طريقة رائعة مكنتنا من ارسال ترددات تصل الي 1000 ميجا بت لكل ثانية علي كابل ذو مدي ترددي 100 هرتز اي من خلال كابل من الفئة الخامسة ومشتقاتها cat 5





لا شك أن لكل مشكلة حل ، ويمكن حل المشكلة بسهولة إذا تم معرفة السبب . حيث أن اكتشاف المشكلة وإصلاحها بدقة وبسرعة لا يكون بمحض الصدفة فحسب ، وإنما يتطلب اتباع إجراءات محددة . وفي مجال الشبكات ، هناك خطوات فنية يجب اتباعها بالترتيب ، ولا بد أن تعرف تفاصيل كل خطوة وما عليك أن تفعله فيها لتتمكن من الانتقال للخطوة التي تليها ، حتى تصل للخطوة الأخيرة وبها تكون المهمة اكتملت وأنك متأكد من سلامة وفاعلية العمل الذي قمت به

في هذا المقال ، سوف نتحدث عن الخطوات التسع والتي تعتمدها منظمة CompTIA في منهاج شهادة Network + كمنهجية لحل مشاكل الشبكة .

- جمْع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة .
- تحديد الأماكن التي بها عطل في الشبكة .
- معرفة أخر التغييرات في الشبكة .
- تكوين فكرة عن أكثر سبب محتمل .
- قد تحتاج إلى رفع المشكلة إلى سُلطة تنفيذية أعلى إذا كانت المشكلة خارج مسؤوليتك .
- وضع خطة عمل للبدء بالحل ، مع الأخذ بالاعتبار تحديد التأثيرات الكامنة وراء كل خطوة .
- تنفيذ الحل ، ثم اختبار فاعليته بتفحص الأجزاء التي كانت متضررة .
- معرفة نتائج التفحص وتأثيرات الحل .
- وأخيرا ، سجّل الحل بكتابة تقرير عن كامل العملية .

الخطوة (1): جَمْع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة

تكون الخطوة الأولى في عملية إصلاح المشكلة هي معرفة المشكلة الموجودة من خلال العلامات التي تدل عليها . ولكي تحصل على المعلومات فإنه يجب أن يكون لديك معرفة بنظام التشغيل المُستخْدم ، ومهارات التواصل الشخصية ، وشيئا من الصبر .

هناك ثلاثة مصادر رئيسية تستطيع أن تجمع منها المعلومات ، وهي :

+++ جهاز الكمبيوتر +++

وذلك عن طريق رسائل الخطأ التي يظهرها النظام عندما تحصل المشكلة ، ويمكن تفسير هذه الرسائل من خلال مراجعة الويب سايت (Website) للشركة المُصنعة لنظام التشغيل المثبت على جهاز الكمبيوتر .

+++ الشخص الذي لديه المشكلة +++

تُعتبر مهارات التواصل الفعّال مع المستخدم ذات أهمية كبيرة عند جمع المعلومات ، وفي غالب الأحيان يكون المستخدم ذو معرفة محدودة بالكمبيوتر وهذا يجعل الأمر أكثر صعوبة لمعرفة ماهِية المشكلة ، ولكن من خلال مقابلة المستخدم وطرح عليه بعض الأسئلة فإنه سوف يخبرك ماذا حدث ، وما كان يحاول أن يفعله ، وما هي الأمور التي لا تعمل .

وأهم المعلومات التي يجب أن تسأل عنها في هذه المقابلة هي :

/// مرات تكرُّر الخطأ :

هل يحدث الخطأ على فترات منتظمة أم بشكل متقطع هل يحصل يومياً أم أسبوعياً أم شهرياً ؟

/// التطبيقات المستخدمة :

من المهم أن تعرف ما هي البرامج التي كانت تعمل وقت حدوث المشكلة .

منهجية حل مشاكل الشبكة

منهجية حل مشاكل الشبكة

علاء مازن عدي

الجزء الأول

/// المشكلات الماضية:

هل حدثت هذه المشكلة من سابق ؟ هل كان لها علاقة بإحدى المشكلات قد حصلت في الماضي ؟

/// تغييرات من المُستخدِم:

إضافة أو إزالة برنامج أو أحد مكونات الكمبيوتر قد يكون له تأثير سلبي على أمور أخرى كانت تعمل بشكل سليم من قبل . استفسر من المستخدم فيما إذا فعل أي تغييرات في الجهاز .

/// رسائل الخطأ:

تعرض أنظمة التشغيل رسائل خطأ لإبلاغ المستخدم بالمشكلة الحاصلة في هذا الوقت .

اسأل المستخدم لكي يخبرك ما هي الرسالة التي تظهر له .

+++ خبرتك وملاحظاتك الشخصية +++

تلعب أساليب الملاحظة الفنية باستخدام حاسة النظر والسمع والشم دوراً كبيراً في عملية اكتشاف الخطأ ، وبذلك فإنك تستطيع أن تجد المشكلة وهي صغيرة قبل أن تصبح مشكلة كبيرة .

وكمثال على هذه النقطة ، مشكلة انفصال الكيبل المتصل بكرت الشبكة فإنك سوف تلاحظ انطفاء أزرار الضوء (LED) الموجودة على جانبي منفذ الكرت ، وعند قيامك بإعادة تثبيته جيداً فسترى أن هذه الأزرار تومض دليل على أن التوصيل صحيح والاتصال يعمل بشكل سليم .

❋❋❋ أسئلة عملية ذات أهمية ❋❋❋

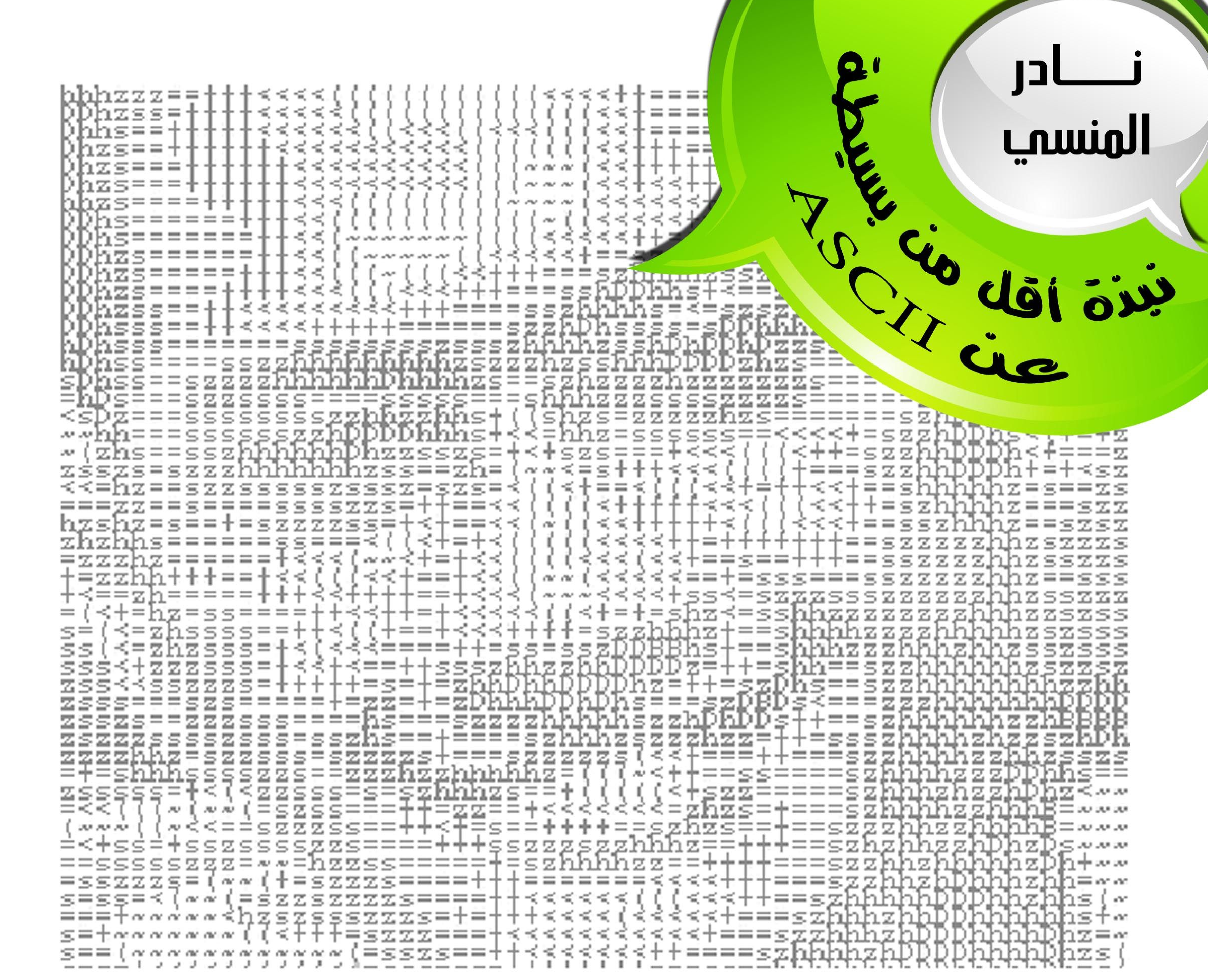
بغض النظر عن الطريقة التي تستخدمها لجمع المعلومات عن المشكلة الحاصلة ، يجب أن تبحث عن إجابات لبعض الأسئلة الهامة .

عندما تبحث في مشكلة تأكد من معرفة إجابات الأسئلة التالية لكي تصل لجذر المشكلة :

- هل المشكلة تخص جهاز كمبيوتر واحد أم أن كامل الشبكة معطلة ؟
- هل هناك مشكلة في تصفح موقع معين ؟ أو نوع معين (أي ftp ، https ، http) ؟
- هل يمكنك عمل ping للتأكد من سلامة اتصالك بالجهاز الآخر ؟
- هل تأكدت من إعدادات الاتصال من خلال الأمر ipconfig /all ؟
- هل المشكلة تحدث باستمرار أم أنها متقطعة ؟ وهل لها أوقات معينة ؟
- هل حدثت نفس المشكلة من قبل ؟
- هل تم إزالة أو تركيب أي من معدات الشبكة حديثا ؟
- هل تم تثبيت أي تطبيقات جديدة على الشبكة ؟
- هل حاول أحد ما إصلاح المشكلة ؟ إذا كان كذلك ، فماذا فعل ؟
- هل يوجد أي مستندات أو تقارير سابقة تتعلق بالمشكلة أو بالتطبيقات أو الأجهزة المرتبطة بالمشكلة ؟

عندما تجد الإجابة على هذه التساؤلات فإنك بذلك تكون كوّنت فكرة أفضل عن حقيقة المشكلة الموجودة بالضبط . وبهذا فإن المرحلة الأولى قد انتهت ويأتي بعدها دور المرحلة الثانية .

في العدد القادم سوف نكمل حديثنا بإذن الله عن الخطوات الأخرى .... دمتم بخير ....



يعتبر الجبر البوليني هو الأب الشرعي للتكنولوجيا الرقمية التي انبثق منها الكمبيوتر و تكنولوجيا الإتصالات الحديثة , و تتمحور فكرة الجبر البوليني هو تحويل أي رقم الي رقمين فقط هما 0 و 1

و بتبسيط أكثر و بعيدا عن الجبر البوليني , هو تحويل أي شيء في هذه الدنيا الي احتمالين فقط هما نعم أو لا – ابيض او اسود ,, أو اي احتمالين متضادين لا ثالث لهما كـ مغلق مفتوح – فوق تحت – يمين يسار و يتم تقريب اي احتمال أخر الي هذين الإحتمالين

تصور مثلا بعد أن كنت تتعامل مع الف لغة تترجم بينهم ثم تفاجأ انك ستتعامل فقط مع لغتين ,, أظن أنك سيغمي عليك من الفرحة

حيث تتمثل الألف لغة في الحروف و الأرقام بكل لغات العالم مع أشكال الصور و الفيديو و كل شيء ,, هذا كله سيتم تحويلة بطريقة ما الي رقمين فقط أو احتمالين فقط هما 0 , 1

هل الأمر بهذه البساطة ؟ لا اطلاقا لكن تكفيك هذه الأساسيات لتفهم سر النمو الغير طبيعي لتكنولوجيا الإتصالات و المعلومات و الألكترونيات

فقد كانت هذه الفرضيات أو النظريات أساس ما تراه حاليا من تكنولوجيا و تم استغلالها فيزيائيا و تحويرها الي اجهزة و الالات لا مجال لسرد طريقة عملها في صفحات

نبذة أقل من بسيطة عن ASCII

و غالبا و بما انك تقرأ هذا الموضوع و وصلت غير مجبرا الي هذا السطر فأنت علي علم بأساسيات التحويل بين الأرقام العادية و ألرقام الثنائية او التحويل بين النظام التماثلي الي النظام الرقمي و لكن ربما يغيب عنك تحويل الحروف الي هذا النظام

و التحويل من الحروف الي النظام الرقمي كي تستطيع الأجهزة الرقمية التعامل معه يتم بإستخدام طريقة تحويل تسمي the American Standard Code for Information Interchange ASCII CODE النظام الأمريكي للتحويل وفق الجدول التالي :

ASCII TABLE

Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]
1	1	1	1	[START OF HEADING]
2	2	10	2	[START OF TEXT]
3	3	11	3	[END OF TEXT]
4	4	100	4	[END OF TRANSMISSION]
5	5	101	5	[ENQUIRY]
6	6	110	6	[ACKNOWLEDGE]
7	7	111	7	[BELL]
8	8	1000	10	[BACKSPACE]
9	9	1001	11	[HORIZONTAL TAB]
10	A	1010	12	[LINE FEED]
11	B	1011	13	[VERTICAL TAB]
12	C	1100	14	[FORM FEED]
13	D	1101	15	[CARRIAGE RETURN]
14	E	1110	16	[SHIFT OUT]
15	F	1111	17	[SHIFT IN]
16	10	10000	20	[DATA LINK ESCAPE]
17	11	10001	21	[DEVICE CONTROL 1]
18	12	10010	22	[DEVICE CONTROL 2]
19	13	10011	23	[DEVICE CONTROL 3]
20	14	10100	24	[DEVICE CONTROL 4]
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]
22	16	10110	26	[SYNCHRONOUS IDLE]
23	17	10111	27	[ENG OF TRANS. BLOCK]
24	18	11000	30	[CANCEL]
25	19	11001	31	[END OF MEDIUM]
26	1A	11010	32	[SUBSTITUTE]
27	1B	11011	33	[ESCAPE]
28	1C	11100	34	[FILE SEPARATOR]
29	1D	11101	35	[GROUP SEPARATOR]
30	1E	11110	36	[RECORD SEPARATOR]
31	1F	11111	37	[UNIT SEPARATOR]
32	20	100000	40	[SPACE]
33	21	100001	41	!
34	22	100010	42	"
35	23	100011	43	#
36	24	100100	44	$
37	25	100101	45	%
38	26	100110	46	&
39	27	100111	47	'
40	28	101000	50	(
41	29	101001	51	)
42	2A	101010	52	*
43	2B	101011	53	+
44	2C	101100	54	,
45	2D	101101	55	-
46	2E	101110	56	.
47	2F	101111	57	/

Decimal	Hexadecimal	Binary	Octal	Char
48	30	110000	60	0
49	31	110001	61	1
50	32	110010	62	2
51	33	110011	63	3
52	34	110100	64	4
53	35	110101	65	5
54	36	110110	66	6
55	37	110111	67	7
56	38	111000	70	8
57	39	111001	71	9
58	3A	111010	72	:
59	3B	111011	73	;
60	3C	111100	74	<
61	3D	111101	75	=
62	3E	111110	76	>
63	3F	111111	77	?
64	40	1000000	100	@
65	41	1000001	101	A
66	42	1000010	102	B
67	43	1000011	103	C
68	44	1000100	104	D
69	45	1000101	105	E
70	46	1000110	106	F
71	47	1000111	107	G
72	48	1001000	110	H
73	49	1001001	111	I
74	4A	1001010	112	J
75	4B	1001011	113	K
76	4C	1001100	114	L
77	4D	1001101	115	M
78	4E	1001110	116	N
79	4F	1001111	117	O
80	50	1010000	120	P
81	51	1010001	121	Q
82	52	1010010	122	R
83	53	1010011	123	S
84	54	1010100	124	T
85	55	1010101	125	U
86	56	1010110	126	V
87	57	1010111	127	W
88	58	1011000	130	X
89	59	1011001	131	Y
90	5A	1011010	132	Z
91	5B	1011011	133	[
92	5C	1011100	134	\
93	5D	1011101	135	]
94	5E	1011110	136	^
95	5F	1011111	137	_

Decimal	Hexadecimal	Binary	Octal	Char
96	60	1100000	140	`
97	61	1100001	141	a
98	62	1100010	142	b
99	63	1100011	143	c
100	64	1100100	144	d
101	65	1100101	145	e
102	66	1100110	146	f
103	67	1100111	147	g
104	68	1101000	150	h
105	69	1101001	151	i
106	6A	1101010	152	j
107	6B	1101011	153	k
108	6C	1101100	154	l
109	6D	1101101	155	m
110	6E	1101110	156	n
111	6F	1101111	157	o
112	70	1110000	160	p
113	71	1110001	161	q
114	72	1110010	162	r
115	73	1110011	163	s
116	74	1110100	164	t
117	75	1110101	165	u
118	76	1110110	166	v
119	77	1110111	167	w
120	78	1111000	170	x
121	79	1111001	171	y
122	7A	1111010	172	z
123	7B	1111011	173	{
124	7C	1111100	174	|
125	7D	1111101	175	}
126	7E	1111110	176	~
127	7F	1111111	177	[DEL]

للعلم فالأسكي قادر أيضا علي صياغة الصور و الفيديو و الصوتيات و أي صيغة تجدها علي الكمبيوتر